# Unified Manager를 참조하십시오

SANtricity 11.8

NetApp
December 16, 2024

# 목차

# Unified Manager 6를 사용하여 다중 어레이 관리

## 기본 인터페이스

### Unified Manager 인터페이스 개요

Unified Manager는 웹 기반 인터페이스로, 단일 뷰에서 여러 스토리지 어레이를 관리할 수 있습니다.

기본 페이지

Unified Manager에 로그인하면 기본 페이지가 열리고 * Manage - All * 가 표시됩니다. 이 페이지에서는 네트워크에서 검색된 스토리지 배열의 목록을 스크롤하고, 해당 상태를 보고, 단일 배열 또는 어레이 그룹에서 작업을 수행할 수 있습니다.

탐색 사이드바

탐색 사이드바에서 Unified Manager 기능에 액세스할 수 있습니다.

| 영역 | 설명 |
| --- | --- |
| 관리 | 네트워크에서 스토리지 시스템을 검색하고, 어레이에 대한 SANtricity 시스템 관리자를 시작하고, 한 어레이에서 여러 어레이로 설정을 가져오고, 어레이 그룹을 관리합니다. 설정 가져오기 및 스토리지 그룹 생성과 같은 작업을 수행할 스토리지 이름 옆의 확인란을 선택합니다. 각 행의 끝에 있는 줄임표는 이름 바꾸기와 같은 단일 배열의 작업에 대한 인라인 메뉴를 제공합니다. |
| 운영 | 한 어레이에서 다른 어레이로 설정을 가져오는 것과 같은 배치 작업의 진행률을 봅니다.<br>스토리지 배열의 상태가 최적이 아닌 경우 일부 작업을 사용할 수 없습니다. |
| 인증서 관리 | 브라우저와 클라이언트 간 인증을 위한 인증서를 관리합니다. |
| 액세스 관리 | Unified Manager 인터페이스에 대한 사용자 인증 설정 |
| 지원 | 기술 지원 옵션, 리소스 및 연락처를 봅니다. |

인터페이스 설정 및 도움말

인터페이스 오른쪽 상단에서 도움말 및 기타 설명서에 액세스할 수 있습니다. 로그인 이름 옆의 드롭다운에서 사용할 수 있는 관리 옵션에 액세스할 수도 있습니다.

사용자 로그인 및 암호

시스템에 로그인한 현재 사용자가 인터페이스의 오른쪽 상단에 표시됩니다.

사용자 및 암호에 대한 자세한 내용은 다음을 참조하십시오.

- "관리자 암호 보호를 설정합니다"
- "admin 암호를 변경합니다"
- "로컬 사용자 프로필에 대한 암호를 변경합니다"

## 지원되는 브라우저

### Unified Manager는 다양한 유형의 브라우저에서 액세스할 수 있습니다.

다음 브라우저 및 버전이 지원됩니다.

| 브라우저 | 최소 버전 |
| --- | --- |
| Google Chrome | 89 |
| Mozilla Firefox | 80 |
| 사파리 | 14 |
| Microsoft Edge를 참조하십시오 | 90 |

웹 서비스 프록시는 설치되어 브라우저에서 사용할 수 있어야 합니다.

## 관리자 암호 보호를 설정합니다

### 관리자 암호를 사용하여 Unified Manager를 구성하여 무단 액세스로부터 보호해야 합니다.

#### 관리자 암호 및 사용자 프로필

Unified Manager를 처음 시작하면 관리자 암호를 설정하라는 메시지가 표시됩니다. admin 암호를 가진 모든 사용자는 스토리지 배열에 대한 구성을 변경할 수 있습니다.

관리자 암호 외에도 Unified Manager 인터페이스에는 하나 이상의 역할이 매핑되어 있는 사전 구성된 사용자 프로필이 포함되어 있습니다. 자세한 내용은 을 "액세스 관리 작동 방식"참조하십시오.

사용자 및 매핑을 변경할 수 없습니다. 암호만 수정할 수 있습니다. 암호를 변경하려면 다음을 참조하십시오.

- "admin 암호를 변경합니다"
- "로컬 사용자 프로필에 대한 암호를 변경합니다"

#### 세션 시간 초과

단일 관리 세션 중에 암호를 입력하라는 메시지가 한 번만 표시됩니다. 기본적으로 30분 동안 활동이 없으면 세션 시간이 초과되며, 이 경우 암호를 다시 입력해야 합니다. 다른 사용자가 다른 관리 클라이언트에서 소프트웨어에 액세스하고 세션이 진행되는 동안 암호를 변경하는 경우 다음에 구성 작업 또는 보기 작업을 시도할 때 암호를 입력하라는 메시지가 표시됩니다.

보안상의 이유로 소프트웨어가 "잠금" 상태가 되기 5회만 암호를 입력할 수 있습니다. 이 상태에서는 소프트웨어가 후속 암호 시도를 거부합니다. 암호를 다시 입력하기 전에 10분 정도 기다린 후 "정상" 상태로 재설정해야 합니다.

세션 시간 초과를 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다. 자세한 내용은 을 "세션 시간 제한을 관리합니다"참조하십시오.

## admin 암호를 변경합니다

### Unified Manager에 액세스하는 데 사용되는 admin 암호를 변경할 수 있습니다.

시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
- 현재 관리자 암호를 알아야 합니다.

이 작업에 대해

암호를 선택할 때는 다음 지침을 염두에 두십시오.

- 암호는 대/소문자를 구분합니다.
- 후행 공백은 암호가 설정되어 있을 때 암호에서 제거되지 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
- 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 로컬 사용자 역할 * 탭을 선택합니다.
3. 표에서 * admin * 사용자를 선택합니다.

   암호 변경 단추를 사용할 수 있게 됩니다.

4. 암호 변경 * 을 선택합니다.

   암호 변경 대화 상자가 열립니다.

5. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 사용자가 시스템에 액세스하기 위해 암호를 입력하도록 확인란을 선택합니다.
6. 두 필드에 새 암호를 입력합니다.
7. 이 작업을 확인하려면 로컬 관리자 암호를 입력한 다음 * 변경 * 을 클릭합니다.

## 세션 시간 제한을 관리합니다

### Unified Manager에 대한 시간 초과를 구성하여 지정된 시간 이후에 비활성 세션의 연결을 끊을 수 있습니다.

이 작업에 대해

기본적으로 Unified Manager의 세션 제한 시간은 30분입니다. 이 시간을 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다.

스토리지에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하여 액세스 관리를 구성하는 경우 사용자의 SSO 세션이 최대 제한에 도달하면 세션 시간 초과가 발생할 수 있습니다. 이 문제는 System Manager 세션 시간이 초과되기 전에 발생할 수 있습니다.

단계

1. 메뉴 표시줄에서 사용자 로그인 이름 옆에 있는 드롭다운 화살표를 선택합니다.
2. Enable/Disable session timeout * 을 선택합니다.

   Enable/Disable Session Timeout(세션 시간 제한 활성화/비활성화) 대화 상자가 열립니다.
3. 스피너 컨트롤을 사용하여 시간을 분 단위로 늘리거나 줄입니다.

   설정할 수 있는 최소 시간 초과는 15분입니다.

   세션 시간 초과를 비활성화하려면 * 시간 길이 설정… * 확인란의 선택을 취소합니다.
4. 저장 * 을 클릭합니다.

# 지원합니다

## 검색 개요

### 스토리지 리소스를 관리하려면 먼저 네트워크에서 스토리지 어레이를 검색해야 합니다.

어레이를 어떻게 검색합니까**?**

추가/검색 페이지를 사용하여 조직의 네트워크에서 관리할 스토리지 어레이를 찾아서 추가합니다. 여러 어레이를 검색할 수도 있고 단일 어레이를 검색할 수도 있습니다. 이렇게 하려면 네트워크 IP 주소를 입력한 다음 Unified Manager가 해당 범위의 각 IP 주소에 대한 개별 연결을 시도합니다.

자세한 내용:

- "스토리지 검색 시 고려 사항"
- "여러 스토리지 시스템을 검색합니다"
- "단일 스토리지를 검색합니다"

어레이를 어떻게 관리해야 합니까**?**

어레이를 검색하고 나면 * Manage - All * 페이지로 이동합니다. 이 페이지에서는 네트워크에서 검색된 스토리지 배열의 목록을 스크롤하고, 해당 상태를 보고, 단일 배열 또는 어레이 그룹에서 작업을 수행할 수 있습니다.

단일 어레이를 관리하려면 어레이를 선택하고 System Manager를 열 수 있습니다.

자세한 내용:

- "System Manager 액세스에 대한 고려 사항"
- "개별 스토리지 어레이를 관리합니다"

- "스토리지 배열 상태를 봅니다"

## 개념

### 스토리지 검색 시 고려 사항

Unified Manager가 스토리지 리소스를 표시하고 관리하기 전에 먼저 조직의 네트워크에서 관리할 스토리지 어레이를 검색해야 합니다. 여러 어레이를 검색할 수도 있고 단일 어레이를 검색할 수도 있습니다.

#### 여러 스토리지 시스템을 검색하는 중입니다

여러 어레이를 검색하도록 선택한 경우 네트워크 IP 주소 범위를 입력한 다음 Unified Manager가 해당 범위의 각 IP 주소에 대한 개별 연결을 시도합니다. 성공적으로 도달한 스토리지 배열이 검색 페이지에 표시되고 관리 도메인에 추가될 수 있습니다.

#### 단일 스토리지 시스템 검색

단일 어레이를 검색하도록 선택한 경우 스토리지 어레이에서 컨트롤러 중 하나에 대한 단일 IP 주소를 입력한 다음 개별 스토리지 어레이가 추가됩니다.

> Unified Manager는 컨트롤러에 할당된 범위 내에서 단일 IP 주소 또는 IP 주소만 검색하여 표시합니다. 이 단일 IP 주소 또는 IP 주소 범위를 벗어나는 컨트롤러에 할당된 대체 컨트롤러 또는 IP 주소가 있는 경우 Unified Manager는 이를 검색 또는 표시하지 않습니다. 그러나 스토리지 배열을 추가하면 연결된 모든 IP 주소가 검색되어 관리 보기에 표시됩니다.

#### 사용자 자격 증명

검색 프로세스 중에 추가할 각 스토리지 배열에 대해 관리자 암호를 제공해야 합니다.

#### 웹 서비스 인증서

검색 프로세스의 일부로 Unified Manager는 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. Unified Manager에서는 브라우저에 설정한 모든 연결에 대해 두 가지 유형의 인증서 기반 인증을 사용합니다.

- * 신뢰할 수 있는 인증서 *

  Unified Manager에서 검색된 스토리지의 경우 인증 기관에서 제공하는 신뢰할 수 있는 인증서를 추가로 설치해야 할 수 있습니다.

  이러한 인증서를 가져오려면 * 가져오기 * 버튼을 사용합니다. 이전에 이 어레이에 연결한 경우 하나 또는 두 컨트롤러 인증서 중 하나가 만료되었거나 해지되었거나 인증서 체인에 루트 인증서 또는 중간 인증서가 누락되었습니다. 스토리지 배열을 관리하기 전에 만료되었거나 해지된 인증서를 교체하거나 누락된 루트 인증서 또는 중간 인증서를 추가해야 합니다.

- * 자체 서명된 인증서 *

  자체 서명된 인증서도 사용할 수 있습니다. 관리자가 서명된 인증서를 가져오지 않고 어레이를 검색하려고 하면 Unified Manager에 관리자가 자체 서명된 인증서를 수락할 수 있는 오류 대화 상자가 표시됩니다. 스토리지 시스템의 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 시스템이 Unified Manager에

추가됩니다.

스토리지 배열에 대한 연결을 신뢰하지 않는 경우, Unified Manager에 스토리지 배열을 추가하기 전에 * Cancel * 을 선택하고 스토리지 배열의 보안 인증서 전략을 확인합니다.

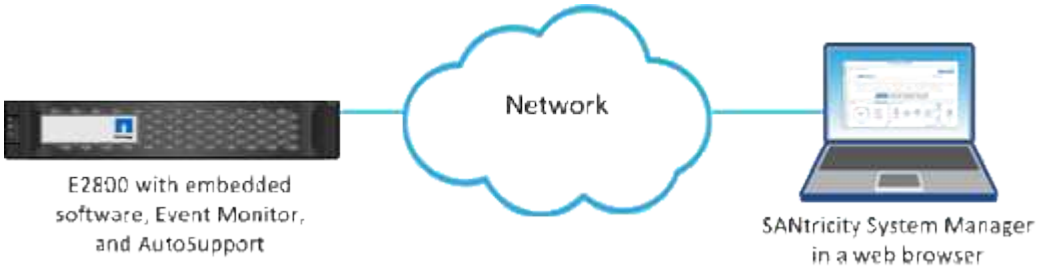
**System Manager** 액세스에 대한 고려 사항

## 스토리지 어레이를 구성 및 관리하려는 경우 하나 이상의 스토리지 어레이를 선택하고 시작 옵션을 사용하여 System Manager를 엽니다.

System Manager는 이더넷 관리 포트를 통해 네트워크에 연결되는 컨트롤러에 내장된 애플리케이션입니다. 모든 스토리지 기반 기능이 포함되어 있습니다.

System Manager에 액세스하려면 다음이 있어야 합니다.

- 여기에 나열된 어레이 모델 중 하나: "E-Series 하드웨어 개요"
- 웹 브라우저를 사용하여 네트워크 관리 클라이언트에 대한 대역외 연결.




## 스토리지를 검색합니다

여러 스토리지 시스템을 검색합니다

## 여러 어레이를 검색하여 관리 서버가 있는 서브넷에서 모든 스토리지 어레이를 검색하고 검색된 어레이를 관리 도메인에 자동으로 추가합니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.
- 스토리지 배열 암호는 System Manager의 액세스 관리 타일을 사용하여 설정해야 합니다.
- 신뢰할 수 없는 인증서를 해결하려면 CA(인증 기관)의 신뢰할 수 있는 인증서 파일이 있어야 하며 로컬 시스템에서 인증서 파일을 사용할 수 있어야 합니다.

어레이 검색 절차는 여러 단계로 이루어진 절차입니다.

**1**단계**:** 네트워크 주소를 입력합니다

로컬 하위 네트워크에서 검색할 네트워크 주소 범위를 입력합니다. 성공적으로 도달한 스토리지 배열이 검색 페이지에 표시되고 관리 도메인에 추가될 수 있습니다.

어떤 이유로든 검색 작업을 중지해야 하는 경우 * 검색 중지 * 를 클릭합니다.

단계

1. 관리 페이지에서 * 추가/검색 * 을 선택합니다.

   추가/검색 대화 상자가 나타납니다.

2. 네트워크 범위 내의 모든 스토리지 배열 검색 * 라디오 버튼을 선택합니다.
3. 로컬 하위 네트워크를 검색할 시작 네트워크 주소와 끝 네트워크 주소를 입력한 다음 * 검색 시작 * 을 클릭합니다.

   검색 프로세스가 시작됩니다. 이 검색 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 스토리지 배열이 검색되면 검색 페이지의 테이블이 채워집니다.

   관리 가능한 어레이가 검색되지 않으면 스토리지 어레이가 네트워크에 올바르게 연결되어 있고 할당된 주소가 범위 내에 있는지 확인합니다. 추가/검색 페이지로 돌아가려면 * New Discovery Parameters * 를 클릭합니다.

4. 검색된 스토리지 시스템의 목록을 검토합니다.
5. 관리 도메인에 추가할 스토리지 배열 옆의 확인란을 선택하고 * 다음 * 을 클릭합니다.

   Unified Manager는 관리 도메인에 추가할 각 어레이에서 자격 증명 검사를 수행합니다. 해당 배열과 연결된 자체 서명된 인증서 및 신뢰할 수 없는 인증서를 확인해야 할 수 있습니다.

6. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

**2**단계**:** 검색 중에 자체 서명된 인증서 해결

검색 프로세스의 일부로 시스템은 스토리지 어레이가 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다.

단계

1. 다음 중 하나를 수행합니다.
   - 검색된 스토리지 배열에 대한 접속을 신뢰할 수 있는 경우 마법사의 다음 카드로 계속 진행합니다. 자체 서명된 인증서는 신뢰할 수 있는 인증서로 표시되며 스토리지 시스템이 Unified Manager에 추가됩니다.
   - 스토리지 어레이에 대한 연결을 신뢰할 수 없는 경우 * Cancel * 을 선택하고 각 스토리지 어레이의 보안 인증서 전략을 확인한 다음 Unified Manager에 추가합니다.
2. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

**3**단계**:** 검색 중에 신뢰할 수 없는 인증서를 해결합니다

신뢰할 수 없는 인증서는 스토리지 어레이에서 Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 어레이 검색 프로세스 중에 신뢰할 수 있는 타사에서 발급한 CA(인증 기관) 인증서 또는 CA 서명 인증서를 가져와 신뢰할 수 없는 인증서를 해결할 수 있습니다.

다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

- 최근에 스토리지 배열을 추가했습니다.
- 하나 이상의 인증서가 만료되었습니다.
- 하나 이상의 인증서가 해지되었습니다.
- 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

단계

1. 신뢰할 수 없는 인증서를 확인할 스토리지 배열 옆의 확인란을 선택한 다음  가져오기 버튼을 선택합니다.

   신뢰할 수 있는 인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

2. Browse * 를 클릭하여 스토리지 배열에 대한 인증서 파일을 선택합니다.

   대화 상자에 파일 이름이 표시됩니다.

3. 가져오기 * 를 클릭합니다.

   파일이 업로드되고 검증됩니다.

   > 신뢰할 수 없는 인증서 문제가 해결되지 않은 스토리지 어레이는 Unified Manager에 추가되지 않습니다.

4. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

**4**단계**:** 암호를 입력합니다

관리 도메인에 추가할 스토리지 배열에 대한 암호를 입력해야 합니다.

단계

1. Unified Manager에 추가할 각 스토리지 어레이의 암호를 입력합니다.
2. * 선택 사항: * 그룹에 스토리지 어레이 연결: 드롭다운 목록에서 선택한 스토리지 어레이와 연결할 그룹을 선택합니다.
3. 마침 * 을 클릭합니다.

작업을 마친 후

스토리지 배열이 관리 도메인에 추가되고 선택한 그룹에 연결됩니다(지정된 경우).

> Unified Manager가 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

단일 스토리지를 검색합니다

## 단일 스토리지 배열 추가/검색 옵션을 사용하여 조직의 네트워크에 단일 스토리지 배열을 수동으로 검색하고 추가합니다.

시작하기 전에

- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.
- 스토리지 배열 암호는 System Manager의 액세스 관리 타일을 사용하여 설정해야 합니다.

단계

1. 관리 페이지에서 * 추가/검색 * 을 선택합니다.

   추가/검색 대화 상자가 나타납니다.

2. Discover a single storage array * 라디오 버튼을 선택합니다.

3. 스토리지 배열에 있는 컨트롤러 중 하나의 IP 주소를 입력한 다음 * 검색 시작 * 을 클릭합니다.

   Unified Manager가 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

   지정된 컨트롤러의 IP 주소에 대한 연결이 실패하면 스토리지 어레이에 액세스할 수 없음 메시지가 나타납니다.

4. 메시지가 표시되면 자체 서명된 인증서를 모두 해결합니다.

   검색 프로세스의 일부로 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. 스토리지 배열에 대한 디지털 인증서를 찾을 수 없는 경우 보안 예외를 추가하여 CA(인증 기관)에서 서명하지 않은 인증서를 확인하라는 메시지가 표시됩니다.

5. 메시지가 나타나면 신뢰할 수 없는 인증서를 모두 확인합니다.

   신뢰할 수 없는 인증서는 스토리지 어레이에서 Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 신뢰할 수 있는 제3자가 발급한 CA(인증 기관) 인증서를 가져와 신뢰할 수 없는 인증서를 해결합니다.

6. 다음 * 을 클릭합니다.
7. * 선택 사항: * 검색된 스토리지 배열을 그룹에 연결: 드롭다운 목록에서 스토리지 배열에 연결할 그룹을 선택합니다.

   기본적으로 "모두" 그룹이 선택됩니다.

8. 관리 도메인에 추가할 스토리지 배열의 관리자 암호를 입력한 다음 * 확인 * 을 클릭합니다.

작업을 마친 후

스토리지 시스템이 Unified Manager에 추가되고 지정된 경우 선택한 그룹에 추가됩니다.

자동 지원 데이터 수집이 설정된 경우 추가하는 스토리지 배열에 대한 지원 데이터가 자동으로 수집됩니다.

## 스토리지 관리

스토리지 배열 상태를 봅니다

## Unified Manager는 검색된 각 스토리지 시스템의 상태를 표시합니다.

Manage - All * 페이지로 이동합니다. 이 페이지에서는 웹 서비스 프록시와 해당 스토리지 배열 간의 연결 상태를 볼 수 있습니다.

상태 표시기는 다음 표에 설명되어 있습니다.

| 상태 | 를 나타냅니다 |
| --- | --- |
| 최적 | 스토리지 배열이 Optimal(최적) 상태에 있습니다. 인증서 문제가 없으며 암호가 유효합니다. |
| 암호가 잘못되었습니다 | 잘못된 스토리지 배열 암호가 제공되었습니다. |

| 상태 | 를 나타냅니다 |
| --- | --- |
| 신뢰할 수 없는 인증서입니다 | HTTPS 인증서가 자체 서명되어 있고 가져오지 않았거나 인증서가 CA 서명되었으며 루트 및 중간 CA 인증서를 가져오지 않았기 때문에 스토리지 배열과의 연결을 하나 이상 신뢰할 수 없습니다. |
| 주의가 필요합니다 | 스토리지 어레이에 문제가 있어 수정하려면 스토리지 시스템의 개입이 필요합니다. |
| 잠금 | 스토리지 배열이 잠김 상태에 있습니다. |
| 알 수 없음 | 스토리지 배열에 연결된 적이 없습니다. 웹 서비스 프록시가 시작되고 아직 스토리지 배열과 연결되지 않았거나, 스토리지 배열이 오프라인 상태이고 웹 서비스 프록시가 시작된 이후 연락되지 않은 경우에 이 문제가 발생할 수 있습니다. |
| 오프라인 | 웹 서비스 프록시가 이전에 스토리지 어레이에 연결했지만 이제 모든 연결이 끊어졌습니다. |

개별 스토리지 어레이를 관리합니다

## 실행 옵션을 사용하면 관리 작업을 수행하려는 경우 하나 이상의 스토리지 어레이에 대한 브라우저 기반 System Manager를 열 수 있습니다.

단계

1. 관리 페이지에서 관리할 스토리지 어레이를 하나 이상 선택합니다.
2. 시작 * 을 클릭합니다.

   새 창이 열리고 System Manager 로그인 페이지가 표시됩니다.

3. 사용자 이름과 암호를 입력한 다음 * 로그인 * 을 클릭합니다.

스토리지 배열 암호를 변경합니다

## Unified Manager에서 스토리지 어레이를 보고 액세스하는 데 사용되는 암호를 업데이트할 수 있습니다.

시작하기 전에

- 스토리지 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
- System Manager에서 설정된 스토리지 어레이의 현재 암호를 알아야 합니다.

이 작업에 대해

이 작업에서는 Unified Manager에서 스토리지 어레이에 액세스할 수 있도록 스토리지 어레이의 현재 암호를 입력합니다. System Manager에서 어레이 암호를 변경했으므로 이제는 Unified Manager에서 어레이 암호를 변경해야 할 수도 있습니다.

단계

1. 관리 페이지에서 하나 이상의 스토리지 배열을 선택합니다.

2. SELECT MENU: Uncommon Tasks[스토리지 배열 암호 제공].
3. 각 스토리지 배열의 암호 또는 암호를 입력한 다음 * 저장 * 을 클릭합니다.

**SANtricity Unified Manager**에서 스토리지 어레이를 제거합니다

## Unified Manager에서 더 이상 스토리지 어레이를 관리하지 않으려는 경우 하나 이상의 스토리지 어레이를 제거할 수 있습니다.

이 작업에 대해

제거하는 스토리지 시스템은 액세스할 수 없습니다. 그러나 브라우저를 IP 주소 또는 호스트 이름에 직접 연결하여 제거된 스토리지 배열에 대한 연결을 설정할 수 있습니다.

스토리지 배열을 제거해도 스토리지 배열 또는 해당 데이터에는 어떤 식으로든 영향을 주지 않습니다. 스토리지 배열이 실수로 제거된 경우 다시 추가할 수 있습니다.

단계

1. Manage * 페이지를 선택합니다.
2. 제거할 스토리지 배열을 하나 이상 선택합니다.
3. Uncommon Tasks [Remove storage array] 메뉴를 선택합니다.

   스토리지 어레이가 SANtricity Unified Manager의 모든 보기에서 제거됩니다.

# 설정을 가져옵니다

## 설정 가져오기 개요

## 설정 가져오기 기능을 사용하면 한 어레이에서 여러 어레이로 설정을 가져오기 위한 일괄 작업을 수행할 수 있습니다. 이 기능을 사용하면 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약할 수 있습니다.

가져올 수 있는 설정은 무엇입니까**?**

알림 방법, AutoSupport 구성, 디렉토리 서비스 구성, 스토리지 구성(예: 볼륨 그룹 및 풀) 및 시스템 설정(예: 자동 로드 밸런싱)을 가져올 수 있습니다.

자세한 내용:

- "가져오기 설정 작동 방식"
- "스토리지 구성 복제 요구 사항"

일괄 불러오기는 어떻게 수행합니까**?**

소스로 사용할 스토리지 배열에서 System Manager를 열고 원하는 설정을 구성합니다. 그런 다음 Unified Manager에서 관리 페이지로 이동하여 설정을 하나 이상의 어레이로 가져옵니다.

자세한 내용:

- "알림 설정을 가져옵니다"
- "AutoSupport 설정을 가져옵니다"
- "디렉터리 서비스 설정을 가져옵니다"
- "스토리지 구성 설정을 가져옵니다"
- "시스템 설정을 가져옵니다"

## 개념

### 가져오기 설정 작동 방식

Unified Manager를 사용하여 한 스토리지 어레이에서 여러 스토리지 어레이로 설정을 가져올 수 있습니다. 설정 가져오기 기능은 네트워크에 여러 어레이를 구성해야 할 때 시간을 절약할 수 있는 일괄 작업입니다.

#### 가져올 수 있는 설정입니다

다음 구성을 여러 어레이로 가져올 수 있습니다.

- * Alerts * — e-메일, syslog 서버 또는 SNMP 서버를 사용하여 중요한 이벤트를 관리자에게 보내는 경고 방법입니다.
- * AutoSupport * — 스토리지 어레이의 상태를 모니터링하고 자동 디스패치를 기술 지원 부서에 보내는 기능입니다.
- * 디렉터리 서비스 * — LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스(예: Microsoft의 Active Directory)를 통해 관리되는 사용자 인증 방법입니다.
- * 스토리지 구성 * — 다음과 관련된 구성:
  - 볼륨(일반 및 비리포지토리 볼륨만 해당)
  - 볼륨 그룹 및 풀
  - 핫 스페어 드라이브 할당
- * 시스템 설정 * — 다음과 관련된 구성:
  - 볼륨에 대한 미디어 스캔 설정입니다
  - SSD 설정
  - 자동 로드 밸런싱(호스트 연결 보고 포함 안 함)

#### 구성 워크플로우

설정을 가져오려면 다음 워크플로를 따릅니다.

1. 소스로 사용할 스토리지 배열에서 System Manager를 사용하여 설정을 구성합니다.
2. 타겟으로 사용할 스토리지 어레이에서 System Manager를 사용하여 구성을 백업합니다.
3. Unified Manager에서 * 관리 * 페이지로 이동하여 설정을 가져옵니다.
4. Operations * 페이지에서 설정 가져오기 작업의 결과를 검토합니다.

스토리지 구성 복제 요구 사항

## 스토리지 시스템 간에 스토리지 구성을 가져오기 전에 요구 사항 및 지침을 검토하십시오.

쉘프

- 컨트롤러가 상주하는 쉘프는 소스 및 타겟 어레이에서 동일해야 합니다.
- 소스 및 타겟 스토리지에서 쉘프 ID가 동일해야 합니다.
- 확장 쉘프가 동일한 드라이브 유형으로 동일한 슬롯에 설치되어야 합니다(구성에서 드라이브를 사용하는 경우, 사용되지 않은 드라이브의 위치는 중요하지 않음).

컨트롤러

- 컨트롤러 유형은 소스 어레이와 타겟 어레이 간에 다를 수 있지만(예: E2800에서 E5700으로 가져오기) RBOD 케이스 유형은 동일해야 합니다.
- 호스트의 DA 기능을 포함한 HIC는 소스와 타겟 스토리지 간에 동일해야 합니다.
- 양면 인쇄에서 단면 인쇄로 가져오는 것은 지원되지 않지만 단면 인쇄에서 양면 인쇄로 가져오는 것은 허용됩니다.
- FDE 설정은 가져오기 프로세스에 포함되지 않습니다.

상태

- 타겟 스토리지가 최적 상태여야 합니다.
- 소스 스토리지가 최적 상태가 아니어야 합니다.

스토리지

- 타겟의 볼륨 용량이 소스보다 큰 경우 소스 스토리지와 타겟 스토리지 간에 드라이브 용량이 다를 수 있습니다. (타겟 스토리지에는 복제 작업에 의해 볼륨으로 완전히 구성되지 않는 더 큰 최신 용량 드라이브가 있을 수 있습니다.)
- 소스 스토리지에서 64TB 이상의 디스크 풀 볼륨으로 인해 타겟의 가져오기 프로세스가 실행되지 않습니다.
- 씬 볼륨은 가져오기 프로세스에 포함되지 않습니다.

## 일괄 가져오기를 사용합니다

알림 설정을 가져옵니다

## 한 스토리지 어레이에서 다른 스토리지 어레이로 경고 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 알림은 소스로 사용할 스토리지 어레이에 대해 System Manager에서 구성됩니다(메뉴: 설정 [경고]).
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져오기 작업에 대한 e-메일, SNMP 또는 syslog 알림을 선택할 수 있습니다. 가져온 설정은 다음과 같습니다.

- * 이메일 경고 * — 메일 서버 주소 및 경고 수신자의 이메일 주소입니다.
- Syslog 경고 * — syslog 서버 주소와 UDP 포트입니다.
- SNMP 경고 * — SNMP 서버의 커뮤니티 이름 및 IP 주소입니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 이메일 경고 *, * SNMP 경고 * 또는 * Syslog 경고 * 를 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

   8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 e-메일, SNMP 또는 syslog를 통해 관리자에게 알림을 보내도록 타겟 스토리지 시스템을 구성할 수 있습니다.

### **AutoSupport** 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 AutoSupport 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 소스로 사용할 스토리지 어레이에 대한 AutoSupport가 시스템 관리자에 구성됩니다(메뉴: 지원 [지원 센터]).
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져온 설정에는 별도 기능(기본 AutoSupport, AutoSupport OnDemand 및 원격 진단), 유지 관리 창, 제공 방법, 및 발송 일정을 참조하십시오.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * AutoSupport * 를 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

   8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 AutoSupport 설정으로 구성됩니다.

디렉터리 서비스 설정을 가져옵니다

## 한 스토리지 어레이에서 다른 스토리지 어레이로 디렉토리 서비스 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 디렉토리 서비스는 소스로 사용할 스토리지 어레이에 대해 System Manager에서 구성됩니다(메뉴: 설정 [액세스 관리]).
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져온 설정에는 LDAP(Lightweight Directory Access Protocol) 서버의 도메인 이름과 URL, LDAP 서버의 사용자 그룹에 대한 매핑과 스토리지 배열의 사전 정의된 역할에 대한 URL이 포함됩니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 디렉터리 서비스 * 를 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 디렉토리 서비스로 구성됩니다.

시스템 설정을 가져옵니다

## 한 스토리지 어레이에서 다른 스토리지 어레이로 시스템 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 시스템 설정은 소스로 사용할 스토리지 배열에 대해 System Manager에서 구성됩니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져온 설정에는 볼륨에 대한 미디어 스캔 설정, 컨트롤러에 대한 SSD 설정, 자동 로드 밸런싱(호스트 연결 보고 제외)이 포함됩니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 시스템 * 을 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 시스템 설정으로 구성됩니다.

## 스토리지 구성 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 스토리지 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 스토리지는 소스로 사용할 스토리지 배열에 대해 SANtricity System Manager에서 구성됩니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.
- 소스 및 타겟 스토리지가 다음 요구 사항을 충족해야 합니다.
  - 컨트롤러가 상주하는 쉘프는 동일해야 합니다.
  - 쉘프 ID는 동일해야 합니다.
  - 확장 셸프는 동일한 드라이브 유형으로 동일한 슬롯에 설치되어야 합니다.
  - RBOD 케이스 유형은 동일해야 합니다.
  - 호스트의 Data Assurance 기능을 비롯한 HIC는 동일해야 합니다.
  - 타겟 스토리지가 최적 상태여야 합니다.
  - 타겟 스토리지의 볼륨 용량이 소스 스토리지의 용량보다 큽니다.
- 다음과 같은 제한 사항을 이해합니다.
  - 양면 인쇄에서 단면 인쇄로 가져오는 것은 지원되지 않지만 단면 인쇄에서 양면 인쇄로 가져오는 것은 허용됩니다.
  - 소스 스토리지에서 64TB 이상의 디스크 풀 볼륨으로 인해 타겟의 가져오기 프로세스가 실행되지 않습니다.
  - 씬 볼륨은 가져오기 프로세스에 포함되지 않습니다.

이 작업에 대해

가져온 설정에는 구성된 볼륨(일반 및 비리포지토리 볼륨만 해당), 볼륨 그룹, 풀 및 핫 스페어 드라이브 할당이 포함됩니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 스토리지 구성 * 을 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 스토리지 구성으로 구성됩니다.

## FAQ 를 참조하십시오

가져올 설정은 무엇입니까?

### 설정 가져오기 기능은 하나의 스토리지 어레이에서 여러 스토리지 어레이로 구성을 로드하는 일괄 작업입니다. 이 작업 중에 가져오는 설정은 소스 스토리지 배열이 System Manager에 구성된 방식에 따라 다릅니다.

다음 설정을 여러 스토리지 어레이로 가져올 수 있습니다.

- * 이메일 경고 * — 설정에는 메일 서버 주소와 경고 받는 사람의 이메일 주소가 포함됩니다.
- * Syslog alerts * — 설정에는 syslog 서버 주소와 UDP 포트가 포함됩니다.
- SNMP 경고 * — 설정에는 SNMP 서버에 대한 커뮤니티 이름과 IP 주소가 포함됩니다.
- * AutoSupport * — 설정에는 별도 기능(기본 AutoSupport, AutoSupport OnDemand 및 원격 진단), 유지보수 윈도우, 제공 방법, 및 발송 일정을 참조하십시오.
- * 디렉토리 서비스 * — 구성에는 LDAP(Lightweight Directory Access Protocol) 서버의 도메인 이름 및 URL과 LDAP 서버의 사용자 그룹에 대한 스토리지 배열의 사전 정의된 역할에 대한 매핑이 포함됩니다.
- * 스토리지 구성 * — 구성에는 볼륨(일반 및 비리포지토리 볼륨만), 볼륨 그룹, 풀 및 핫 스페어 드라이브 할당이 포함됩니다.
- * 시스템 설정 * — 구성에는 볼륨에 대한 미디어 스캔 설정, 컨트롤러에 대한 SSD 캐시, 자동 로드 밸런싱(호스트 연결 보고 제외)이 포함됩니다.

내 스토리지 어레이가 모두 보이지 않는 이유는 무엇입니까?

### 설정 가져오기 작업 중에 일부 스토리지 배열을 대상 선택 대화 상자에서 사용하지 못할 수 있습니다.

다음과 같은 이유로 스토리지 어레이가 나타나지 않을 수 있습니다.

- 펌웨어 버전이 8.50 미만입니다.
- 스토리지 배열이 오프라인입니다.
- 시스템이 해당 어레이와 통신할 수 없습니다(예: 어레이에 인증서, 암호 또는 네트워킹 문제가 있음).

# 스토리지 그룹

## 그룹 개요

### Manage Groups 페이지에서 스토리지 어레이 그룹 세트를 생성하여 관리를 간소화할 수 있습니다.

어레이 그룹이란 무엇입니까**?**

스토리지 시스템 세트를 그룹화하여 물리적 인프라와 가상화 인프라를 관리할 수 있습니다. 모니터링 또는 보고 작업을 보다 쉽게 실행할 수 있도록 스토리지 어레이를 그룹화할 수 있습니다.

두 가지 유형의 그룹이 있습니다.

- * All group * — all 그룹은 기본 그룹이며 조직에서 검색된 모든 스토리지 어레이를 포함합니다. All(모두) 그룹은 기본 보기에서 액세스할 수 있습니다.
- * 사용자 생성 그룹 * — 사용자 생성 그룹에는 해당 그룹에 추가하기 위해 수동으로 선택한 스토리지 배열이 포함됩니다. 사용자 생성 그룹은 기본 보기에서 액세스할 수 있습니다.

그룹을 구성하려면 어떻게 합니까**?**

그룹 관리 페이지에서 그룹을 생성한 다음 해당 그룹에 어레이를 추가할 수 있습니다.

자세한 내용:

- "스토리지 어레이 그룹을 구성합니다"

## 스토리지 어레이 그룹을 구성합니다

### 스토리지 그룹을 생성한 다음 스토리지 시스템을 그룹에 추가합니다.

그룹 구성은 2단계 절차입니다.

**1**단계**:** 그룹 만들기

먼저 그룹을 만듭니다. 스토리지 그룹은 볼륨을 구성하는 스토리지를 제공하는 드라이브를 정의합니다.

단계

1. 관리 페이지에서 메뉴 관리 그룹 [스토리지 그룹 생성]을 선택합니다.
2. 이름 * 필드에 새 그룹의 이름을 입력합니다.
3. 새 그룹에 추가할 스토리지 배열을 선택합니다.
4. Create * 를 클릭합니다.

**2**단계**:** 스토리지 배열을 그룹에 추가합니다

사용자가 생성한 그룹에 하나 이상의 스토리지 어레이를 추가할 수 있습니다.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 스토리지 배열을 추가할 그룹을 선택합니다.
2. 메뉴: Manage Groups [Add storage arrays to group]를 선택합니다.
3. 그룹에 추가할 스토리지 배열을 선택합니다.
4. 추가 * 를 클릭합니다

## 그룹에서 스토리지 배열을 제거합니다

### 특정 스토리지 그룹에서 더 이상 관리 대상 스토리지 어레이를 관리하지 않으려는 경우 그룹에서 하나 이상의 관리되는 스토리지 어레이를 제거할 수 있습니다.

이 작업에 대해

그룹에서 스토리지 배열을 제거해도 스토리지 배열 또는 해당 데이터에는 어떤 식으로든 영향을 주지 않습니다. System Manager에서 스토리지 어레이를 관리하는 경우에도 브라우저를 사용하여 관리할 수 있습니다. 스토리지 배열이 그룹에서 실수로 제거된 경우 다시 추가할 수 있습니다.

단계

1. 관리 페이지에서 메뉴 관리 그룹 [그룹에서 스토리지 배열 제거]를 선택합니다.
2. 드롭다운에서 제거할 스토리지 배열이 포함된 그룹을 선택한 다음 그룹에서 제거할 각 스토리지 배열 옆의 확인란을 클릭합니다.
3. 제거 * 를 클릭합니다.

## 스토리지 어레이 그룹을 삭제합니다

### 더 이상 필요하지 않은 스토리지 그룹을 하나 이상 제거할 수 있습니다.

이 작업에 대해

이 작업은 스토리지 어레이 그룹만 삭제합니다. 삭제된 그룹과 연결된 스토리지 배열은 모두 관리 보기 또는 연결된 다른 그룹을 통해 액세스할 수 있습니다.

단계

1. 관리 페이지에서 메뉴 관리 그룹 [스토리지 어레이 그룹 삭제]를 선택합니다.
2. 삭제할 스토리지 그룹을 하나 이상 선택합니다.
3. 삭제 * 를 클릭합니다.

## 스토리지 그룹 이름을 바꿉니다

### 현재 이름이 더 이상 의미가 없거나 적용할 수 없는 경우 스토리지 어레이 그룹의 이름을 변경할 수 있습니다.

이 작업에 대해

이 지침을 염두에 두십시오.

- 이름은 문자, 숫자 및 밑줄(_), 하이픈(-) 및 파운드(#)로 구성될 수 있습니다. 다른 문자를 선택하면 오류 메시지가 나타납니다. 다른 이름을 선택하라는 메시지가 표시됩니다.

- 이름을 30자로 제한합니다. 이름의 선행 및 후행 공백이 삭제됩니다.
- 쉽게 이해하고 기억할 수 있는 독특하고 의미 있는 이름을 사용합니다.
- 나중에 그 의미를 금방 잊어버릴 수 있는 임의 이름이나 이름을 피하십시오.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 이름을 바꿀 스토리지 어레이 그룹을 선택합니다.
2. 메뉴 선택: Manage Groups [Rename storage array group](그룹 관리 [스토리지 배열 그룹 이름 바꾸기]).
3. 그룹 이름 * 필드에 그룹의 새 이름을 입력합니다.
4. 이름 바꾸기 * 를 클릭합니다

# 업그레이드

## 업그레이드 센터 개요

## 업그레이드 센터에서 여러 스토리지 어레이에 대한 SANtricity OS 소프트웨어 및 NVSRAM 업그레이드를 관리할 수 있습니다.

### 업그레이드는 어떻게 작동합니까?

최신 OS 소프트웨어를 다운로드한 다음 하나 이상의 어레이를 업그레이드합니다.

#### 워크플로우 업그레이드

다음 단계에서는 소프트웨어 업그레이드를 수행하기 위한 높은 수준의 워크플로우를 제공합니다.

1. Support 사이트에서 최신 SANtricity OS 소프트웨어 파일을 다운로드합니다(지원 페이지의 Unified Manager에서 링크 사용 가능). 관리 호스트 시스템(브라우저에서 Unified Manager에 액세스하는 호스트)에 파일을 저장한 다음 파일의 압축을 풉니다.
2. Unified Manager에서 SANtricity OS 소프트웨어 파일과 NVSRAM 파일을 리포지토리(파일이 저장되는 웹 서비스 프록시 서버 영역)에 로드합니다. 업그레이드 센터 [SANtricity OS 소프트웨어 업그레이드 또는 업그레이드 센터 > 소프트웨어 저장소 관리] 메뉴에서 파일을 추가할 수 있습니다.
3. 저장소에 파일이 로드되면 업그레이드에 사용할 파일을 선택할 수 있습니다. SANtricity OS 소프트웨어 업그레이드 페이지(메뉴: 업그레이드 센터 [SANtricity OS 소프트웨어 업그레이드])에서 SANtricity OS 소프트웨어 파일과 NVSRAM 파일을 선택합니다. 소프트웨어 파일을 선택하면 호환되는 스토리지 배열 목록이 이 페이지에 표시됩니다. 그런 다음 새 소프트웨어로 업그레이드할 스토리지 어레이를 선택합니다. (호환되지 않는 어레이는 선택할 수 없습니다.)
4. 그런 다음 즉시 소프트웨어 전송 및 활성화를 시작하거나 나중에 활성화할 파일을 준비하도록 선택할 수 있습니다. 업그레이드 프로세스 중에 Unified Manager는 다음 작업을 수행합니다.
   a. 스토리지 배열의 상태 점검을 수행하여 업그레이드가 완료되지 못할 수 있는 조건이 있는지 확인합니다. 상태 확인에 실패한 어레이가 있으면 해당 특정 어레이를 건너뛰고 다른 어레이를 계속 업그레이드할 수 있습니다. 또는 전체 프로세스를 중지하고 통과하지 못한 어레이의 문제를 해결할 수 있습니다.
   b. 각 컨트롤러로 업그레이드 파일을 전송합니다.
   c. 컨트롤러를 재부팅하여 한 번에 하나의 컨트롤러인 새로운 SANtricity OS 소프트웨어를 활성화합니다. 활성화 중에 기존 SANtricity OS 파일이 새 파일로 대체됩니다.

나중에 소프트웨어가 활성화되도록 지정할 수도 있습니다.

### 즉시 또는 단계별 업그레이드

업그레이드를 즉시 활성화하거나 나중에 스테이징할 수 있습니다. 다음과 같은 이유로 나중에 정품 인증을 선택할 수 있습니다.

- * 시간 * — 소프트웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 부하가 더 가벼워질 때까지 기다려야 할 수 있습니다. I/O 로드 및 캐시 크기에 따라 컨트롤러 업그레이드를 완료하는 데 일반적으로 15~25분 정도 걸릴 수 있습니다. 활성화 중에 컨트롤러가 재부팅되고 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
- * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.

스테이징된 소프트웨어를 활성화하려면 메뉴 [업그레이드 센터]로 이동한 후 SANtricity OS 컨트롤러 소프트웨어 업그레이드라고 표시된 영역에서 * 활성화 * 를 클릭합니다.

### 상태 점검

상태 점검은 업그레이드 프로세스의 일부로 실행되지만 시작하기 전에 별도로 상태 점검을 실행할 수도 있습니다(메뉴: 업그레이드 센터 [사전 업그레이드 상태 점검]).

상태 점검을 통해 모든 스토리지 시스템 구성요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다. 다음 조건에서는 업그레이드가 되지 않을 수 있습니다.

- 할당된 드라이브에 오류가 발생했습니다
- 핫 스페어가 사용 중입니다
- 볼륨 그룹이 불완전합니다
- 단독 운영 실행 중
- 볼륨이 누락되었습니다
- 컨트롤러가 최적화되지 않은 상태입니다
- 이벤트 로그 이벤트의 수가 너무 넘습니다
- 구성 데이터베이스 유효성 검사에 실패했습니다
- DACstore의 이전 버전이 있는 드라이브입니다

## 업그레이드하기 전에 알아야 할 사항은 무엇입니까?

여러 스토리지 시스템을 업그레이드하기 전에 계획의 일환으로 주요 고려 사항을 검토하십시오.

### 현재 버전

검색된 각 스토리지 시스템에 대해 Unified Manager의 관리 페이지에서 현재 SANtricity OS 소프트웨어 버전을 확인할 수 있습니다. 이 버전은 SANtricity OS 소프트웨어 열에 표시됩니다. 각 행에서 SANtricity OS 버전을 클릭하면 컨트롤러 펌웨어 및 NVSRAM 정보를 팝업 대화 상자에서 사용할 수 있습니다.

업그레이드가 필요한 기타 구성 요소

업그레이드 프로세스 중에 호스트가 컨트롤러와 올바르게 상호 작용할 수 있도록 호스트의 다중 경로/페일오버 드라이버 또는 HBA 드라이버를 업그레이드해야 할 수도 있습니다.

호환성 정보는 을 "NetApp 상호 운용성 매트릭스"참조하십시오. 또한 운영 체제의 Express Guide에 있는 절차를 참조하십시오. Express 가이드는 에서 "E-Series 및 SANtricity 설명서"제공됩니다.

듀얼 컨트롤러

스토리지 어레이에 2개의 컨트롤러가 포함되어 있고 다중 경로 드라이버가 설치되어 있는 경우, 업그레이드가 진행되는 동안 스토리지 어레이에서 I/O를 계속 처리할 수 있습니다. 업그레이드 중에 다음 프로세스가 발생합니다.

1. 컨트롤러 A는 모든 LUN을 컨트롤러 B로 페일오버합니다
2. 컨트롤러 A에서 업그레이드가 발생합니다
3. 컨트롤러 A는 LUN과 모든 컨트롤러 B의 LUN을 백업합니다.
4. 컨트롤러 B에서 업그레이드가 발생합니다

업그레이드가 완료된 후 컨트롤러 간에 볼륨을 수동으로 재배포하여 볼륨이 올바른 소유 컨트롤러로 돌아가도록 해야 할 수 있습니다.

## 소프트웨어 및 펌웨어를 업그레이드합니다

업그레이드 전 상태 점검을 수행합니다

### 상태 점검은 업그레이드 프로세스의 일부로 실행되지만 시작하기 전에 상태 점검을 별도로 실행할 수도 있습니다. 상태 점검을 통해 스토리지 시스템의 구성 요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 메뉴: 업그레이드 센터 [업그레이드 전 상태 점검] 을 선택합니다.

   업그레이드 전 상태 점검 대화 상자가 열리고 검색된 모든 스토리지 시스템이 나열됩니다.

2. 필요한 경우 현재 최적의 상태가 아닌 모든 시스템을 볼 수 있도록 목록에서 스토리지 시스템을 필터링하거나 정렬합니다.
3. 상태 점검을 통해 실행할 스토리지 시스템의 확인란을 선택합니다.
4. 시작 * 을 클릭합니다.

   상태 점검이 수행되는 동안 대화 상자에 진행 상황이 표시됩니다.

5. 상태 점검이 완료되면 각 행의 오른쪽에 있는 줄임표(...)를 클릭하여 추가 정보를 보고 다른 작업을 수행할 수 있습니다.

> 상태 확인에 실패한 어레이가 있으면 해당 특정 어레이를 건너뛰고 다른 어레이를 계속 업그레이드할 수 있습니다. 또는 전체 프로세스를 중지하고 통과하지 못한 어레이의 문제를 해결할 수 있습니다.

**SANtricity OS**를 업그레이드합니다

# 최신 소프트웨어 및 NVSRAM으로 하나 이상의 스토리지 어레이를 업그레이드하여 모든 최신 기능과 버그 수정을 확인할 수 있습니다. 컨트롤러 NVSRAM은 컨트롤러의 기본 설정을 지정하는 컨트롤러 파일입니다.

시작하기 전에

- 최신 SANtricity OS 파일은 SANtricity 웹 서비스 프록시 및 Unified Manager가 실행 중인 호스트 시스템에서 사용할 수 있습니다.
- 소프트웨어 업그레이드를 지금 또는 나중에 활성화할지 여부를 알 수 있습니다.

  다음과 같은 이유로 나중에 정품 인증을 선택할 수 있습니다.

  - * 시간 * — 소프트웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 부하가 더 가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
  - * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 OS 소프트웨어를 테스트할 수 있습니다.

11.80.x 이상으로 업그레이드하려면 시스템에서 SANtricity OS 11.70.5 를 실행해야 합니다.

이 작업에 대해

```
[NOTE]
====
데이터 손실 또는 스토리지 어레이 손상 위험 - 업그레이드가 진행되는 동안 스토리지 어레이를 변경하지 마십시오. 스토리지 어레이에 대한 전원을 유지합니다.

====
.단계
. 스토리지 어레이에 컨트롤러가 하나만 포함되어 있거나 다중 경로 드라이버를 사용하지 않는 경우 스토리지 어레이에 대한 I/O 작업을 중지하여 응용 프로그램 오류를 방지합니다. 스토리지 어레이에 2개의 컨트롤러가 있는데 다중 경로 드라이버가 설치되어 있는 경우 I/O 작업을 중지할 필요가 없습니다.
. 기본 보기에서 * 관리 * 를 선택한 다음 업그레이드할 스토리지 어레이를 하나 이상 선택합니다.
. 메뉴: 업그레이드 센터 [SANtricity OS 소프트웨어 업그레이드]를 선택합니다.
+
SANtricity OS 소프트웨어 업그레이드 페이지가 나타납니다.

. NetApp Support 사이트에서 로컬 시스템으로 최신 SANtricity OS 소프트웨어 패키지를 다운로드하십시오.
+
.. 소프트웨어 리포지토리에 새 파일 추가 * 를 클릭합니다.
.. 최신 * SANtricity OS 다운로드 * 를 찾는 링크를 클릭합니다.
.. 최신 릴리스 다운로드 * 링크를 클릭합니다.
.. 나머지 지침에 따라 SANtricity OS 파일 및 NVSRAM 파일을 로컬 컴퓨터에 다운로드합니다.
```

+
[NOTE]
====
버전 8.42 이상에서는 디지털 서명된 펌웨어가 필요합니다. 서명되지 않은 펌웨어를 다운로드하려고 하면 오류가 표시되고 다운로드가 중단됩니다.

====
. 컨트롤러를 업그레이드하는 데 사용할 OS 소프트웨어 파일과 NVSRAM 파일을 선택합니다.
+
.. SANtricity OS 소프트웨어 파일 선택 * 드롭다운에서 로컬 컴퓨터에 다운로드한 OS 파일을 선택합니다.
+
여러 개의 파일을 사용할 수 있는 경우 파일이 최신 날짜부터 가장 오래된 날짜순으로 정렬됩니다.

+
[NOTE]
====
소프트웨어 리포지토리는 웹 서비스 프록시와 연결된 모든 소프트웨어 파일을 나열합니다. 사용할 파일이 표시되지 않으면 * 소프트웨어 리포지토리에 새 파일 추가 * 링크를 클릭하여 추가할 OS 파일이 있는 위치를 찾을 수 있습니다.

====
.. NVSRAM 파일 선택 * 드롭다운에서 사용할 컨트롤러 파일을 선택합니다.
+
파일이 여러 개 있는 경우 파일이 최신 날짜부터 가장 오래된 날짜순으로 정렬됩니다.



. Compatible Storage Array 표에서 선택한 OS 소프트웨어 파일과 호환되는 스토리지 배열을 검토한 다음 업그레이드할 스토리지를 선택합니다.
+
** 관리 보기에서 선택했으며 선택한 펌웨어 파일과 호환되는 스토리지 배열은 기본적으로 호환 가능한 스토리지 배열 테이블에서 선택됩니다.
** 선택한 펌웨어 파일로 업데이트할 수 없는 스토리지 배열은 * 호환되지 않음 * 상태로 표시된 호환 가능한 스토리지 배열 테이블에서 선택할 수 없습니다.


. * 선택 사항: * 소프트웨어 파일을 활성화하지 않고 스토리지 어레이로 전송하려면 * OS 소프트웨어를 스토리지 어레이로 전송, 스테이징으로 표시 및 나중에 활성화 * 확인란을 선택합니다.
. 시작 * 을 클릭합니다.
. 지금 활성화할지 아니면 나중에 활성화할지 여부에 따라 다음 중 하나를 수행합니다.
+
** 업그레이드하려는 어레이에서 제안된 OS 소프트웨어 버전을 전송할지 확인하려면 * TRANSFER * 를 입력하고 * TRANSFER * 를 클릭합니다.

+
전송된 소프트웨어를 활성화하려면 업그레이드 센터 [스테이징된 OS 소프트웨어 활성화] 메뉴를 선택합니다.

** 업그레이드 * 를 입력하여 업그레이드하도록 선택한 어레이에서 제안된 OS 소프트웨어 버전을 전송 및 활성화한 다음 * 업그레이드 * 를 클릭합니다.
+
시스템은 업그레이드를 위해 선택한 각 스토리지 어레이로 소프트웨어 파일을 전송한 다음 재부팅을 시작하여 해당 파일을 활성화합니다.

+
업그레이드 작업 중에 다음 작업이 수행됩니다.

+
** 업그레이드 전 상태 점검이 업그레이드 프로세스의 일부로 실행됩니다. 업그레이드 전 상태 점검을 통해 모든 스토리지 시스템 구성 요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다.
** 스토리지 배열에 대한 상태 검사에 실패하면 업그레이드가 중지됩니다. 줄임표(...)를 클릭하고 * 로그 저장 * 을 선택하여 오류를 검토할 수 있습니다. 상태 점검 오류를 재정의하도록 선택한 다음 * 계속 * 을 클릭하여 업그레이드를 진행할 수도 있습니다.
** 업그레이드 전 상태 점검 후 업그레이드 작업을 취소할 수 있습니다.

. * 선택 사항: * 업그레이드가 완료되면 줄임표(...)를 클릭한 다음 * Save Log * 를 선택하여 특정 스토리지 배열에 대해 업그레이드된 항목 목록을 볼 수 있습니다.
+
파일이 브라우저의 다운로드 폴더에 이름으로 `upgrade_log-<date>.json`저장됩니다.

[[IDe18f6d9de6403c6acf04412b792181b2]]
= 스테이징된 OS 소프트웨어를 활성화합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
소프트웨어 파일을 즉시 활성화하거나 더 편리한 시간이 될 때까지 기다릴 수 있습니다. 이 절차에서는 나중에 소프트웨어 파일을 활성화하도록 선택한 것으로 가정합니다.

.이 작업에 대해
펌웨어 파일을 활성화하지 않고 전송할 수 있습니다. 다음과 같은 이유로 나중에 정품 인증을 선택할 수 있습니다.

* * 시간 * -- 소프트웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 부하가 더 가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 재부팅되고 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
* * 패키지 유형 * -- 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.

[NOTE]
====
활성화 프로세스가 시작된 후에는 중지할 수 없습니다.

====
.단계
. 기본 보기에서 * 관리 * 를 선택합니다. 필요한 경우 페이지 맨 위에서 Status 열을 클릭하여 "OS Upgrade(활성화 대기 중)" 상태의 모든 스토리지 어레이를 정렬합니다.
. 소프트웨어를 활성화할 스토리지 어레이를 하나 이상 선택한 다음 메뉴: 업그레이드 센터 [스테이징된 OS 소프트웨어 활성화] 를 선택합니다.
+
업그레이드 작업 중에 다음 작업이 수행됩니다.

+
** 업그레이드 전 상태 점검이 활성화 프로세스의 일부로 실행됩니다. 업그레이드 전 상태 점검을 통해 모든 스토리지 시스템 구성 요소를 평가하여 활성화를 진행할 수 있는지 확인합니다.
** 스토리지 배열에 대한 상태 검사에 실패하면 활성화가 중지됩니다. 줄임표(...)를 클릭하고 * 로그 저장 * 을 선택하여 오류를 검토할 수 있습니다. 상태 점검 오류를 재정의하도록 선택한 다음 * 계속 * 을 클릭하여 활성화를 계속 진행할 수도 있습니다.
** 업그레이드 전 상태 점검 후 활성화 작업을 취소할 수 있습니다. 업그레이드 전 상태 점검이 성공적으로 완료되면 활성화가 발생합니다. 활성화하는 데 걸리는 시간은 스토리지 배열 구성과 활성화 중인 구성 요소에 따라 달라집니다.

. * 선택 사항: * 활성화가 완료된 후 줄임표(...)를 클릭한 다음 * Save Log * 를 선택하여 특정 스토리지 배열에 대해 활성화된 항목 목록을 볼 수 있습니다.
+
파일이 브라우저의 다운로드 폴더에 이름으로 `activate_log-<date>.json`저장됩니다.

[[IDa64f892042a735ab40080968ee5bd711]]
= 소프트웨어 저장소를 관리합니다
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
소프트웨어 리포지토리는 웹 서비스 프록시와 연결된 모든 소프트웨어 파일을 나열합니다.

사용할 파일이 표시되지 않으면 소프트웨어 저장소 관리 옵션을 사용하여 하나 이상의 SANtricity OS 파일을 웹 서비스 프록시 및 Unified Manager가 실행 중인 호스트 시스템으로 가져올 수 있습니다. 소프트웨어 저장소에서 사용 가능한 하나 이상의 SANtricity OS 파일을 삭제하도록 선택할 수도 있습니다.

.시작하기 전에
SANtricity OS 파일을 추가하는 경우 로컬 시스템에서 OS 파일을 사용할 수 있는지 확인합니다.

.단계
. 기본 보기에서 * 관리 * 를 선택한 다음 업그레이드 센터 [소프트웨어 리포지토리 관리] 메뉴를 선택합니다.
+
Manage Software Repository 대화상자가 나타납니다.

. 다음 작업 중 하나를 수행합니다.
+
```
[cols="25h,~"]
|===
| 옵션을 선택합니다 | 이렇게 하세요


 a|
```
가져오기
```
 a|
```
.. 가져오기 * 를 클릭합니다
.. 찾아보기 * 를 클릭한 다음 추가할 OS 파일이 있는 위치로 이동합니다.
+
OS 파일의 파일 이름은 과 `N2800-830000-000.dlp`유사합니다.

.. 추가할 OS 파일을 하나 이상 선택한 다음 * 가져오기 * 를 클릭합니다.




 a|
```
삭제
```
 a|
```
.. 소프트웨어 저장소에서 제거할 OS 파일을 하나 이상 선택합니다.
```

.. 삭제 * 를 클릭합니다.

|===

.결과
가져오기를 선택한 경우 파일이 업로드되고 확인됩니다. 삭제를 선택하면 소프트웨어 저장소에서 파일이 제거됩니다.

[[IDbef491507bb34d2f3ac3b2cb950bf601]]
= 스테이징된 OS 소프트웨어를 지웁니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
대기 중인 버전이 나중에 실수로 활성화되지 않도록 스테이징된 OS 소프트웨어를 제거할 수 있습니다. 스테이징된 OS 소프트웨어를 제거해도 스토리지 어레이에서 실행 중인 현재 버전에는 영향을 주지 않습니다.

.단계
. 기본 보기에서 * 관리 * 를 선택한 다음 메뉴: 업그레이드 센터 [스테이징된 OS 소프트웨어 지우기] 를 선택합니다.
+
준비된 OS 소프트웨어 지우기 대화 상자가 열리고 보류 중인 소프트웨어 또는 NVSRAM이 있는 검색된 모든 스토리지 시스템이 나열됩니다.

. 필요한 경우 스테이징된 소프트웨어가 있는 모든 시스템을 볼 수 있도록 목록에서 스토리지 시스템을 필터링하거나 정렬합니다.
. 선택 취소할 보류 중인 소프트웨어가 있는 스토리지 시스템의 확인란을 선택합니다.
. 지우기 * 를 클릭합니다.
+
작업 상태가 대화 상자에 표시됩니다.

:leveloffset: -1

```
:leveloffset: -1


= 미러링

:leveloffset: +1


[[ID6ceca4c007687cd88aa0d9f92a426d45]]
= 미러링 개요
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
미러링 기능을 사용하여 로컬 스토리지 시스템과 원격 스토리지 시스템 간에 데이터를 비동기식으로 또는 동기식으로 복제합니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====


== 미러링이란 무엇입니까?

SANtricity 애플리케이션에는 두 가지 유형의 미러링, 즉 비동기식과 동기식이 있습니다. 비동기식 미러링은 데이터 볼륨을 필요 시 또는 일정에 따라 복제하여 데이터 손상 또는 손실로 인한 다운타임을 최소화 또는 방지합니다. 동기식 미러링은 데이터 볼륨을 실시간으로 복제하여 지속적인 가용성을 보장합니다.

자세한 내용:

* xref:{relative_path}mirroring-overview.html["미러링의 작동 방식"]
* xref:{relative_path}mirroring-terminology.html["미러링 용어"]




== 미러링을 구성하려면 어떻게 합니까?

Unified Manager에서 비동기식 또는 동기식 미러링을 구성한 다음 System Manager를 사용하여 동기화를 관리합니다.
```

자세한 내용:

* xref:{relative_path}mirroring-configuration-workflow.html["미러링 구성 워크플로우"]
* xref:{relative_path}requirements-for-using-mirroring.html["미러링 사용에 대한 요구사항"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["비동기 미러링 쌍을 생성합니다"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["동기식 미러링 쌍을 생성합니다"]

= 개념

:leveloffset: +1

[[ID134dd7fd07b0f5f43b42ee19f6f9c96e]]
= 미러링의 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Unified Manager에는 SANtricity 미러링 기능을 위한 구성 옵션이 포함되어 있어 관리자가 데이터 보호를 위해 두 스토리지 어레이 간에 데이터를 복제할 수 있습니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====

== 미러링 유형

SANtricity 애플리케이션에는 두 가지 유형의 미러링, 즉 비동기식과 동기식이 있습니다.

비동기식 미러링은 데이터 볼륨을 필요 시 또는 일정에 따라 복제하여 데이터 손상 또는 손실로 인한 다운타임을 최소화 또는 방지합니다. 비동기식 미러링은 특정 시점에 기본 볼륨의 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사합니다. 운영 사이트를 즉시 업데이트할 수 있으며 대역폭이 허용할 경우 보조 사이트를 업데이트할 수 있습니다. 네트워크 리소스를 사용할 수 있게 되면 정보가 캐시되어 나중에 전송됩니다. 이러한 유형의 미러링은 백업 및 아카이빙과 같은

주기적인 프로세스에 이상적입니다.

동기식 미러링은 데이터 볼륨을 실시간으로 복제하여 지속적인 가용성을 보장합니다. 두 스토리지 어레이 중 하나에서 재해가 발생할 경우 중요 데이터의 복사본을 사용할 수 있으므로 RPO(복구 시점 목표)를 달성할 수 있습니다. 복제본은 운영 볼륨에 쓸 때마다 보조 볼륨에 쓰기가 수행되므로 항상 운영 데이터와 동일합니다. 보조 볼륨이 운영 볼륨에서 수행된 변경 사항으로 업데이트될 때까지 호스트에 쓰기가 성공했다는 확인 메시지가 표시되지 않습니다. 이러한 유형의 미러링은 재해 복구와 같은 비즈니스 연속성 목적으로 이상적입니다.

== 미러링 유형의 차이점

다음 표에서는 두 미러링 유형의 주요 차이점을 설명합니다.

[cols="1a,1a,1a"]
|===
| 속성 | 비동기식 | 동기식이다

a|
복제 방법입니다
a|
시점 -- 미러링은 사용자 정의 일정에 따라 필요 시 또는 자동으로 수행됩니다.
a|
연속 -- 미러링은 모든 호스트 쓰기에서 데이터를 복사하여 지속적으로 자동 실행됩니다.

a|
거리
a|
어레이 간 장거리 지원. 일반적으로 거리는 네트워크 및 채널 확장 기술의 성능에 의해서만 제한됩니다.
a|
어레이 간 거리가 짧아집니다. 일반적으로 지연 시간 및 애플리케이션 성능 요구 사항을 충족하려면 로컬 스토리지 어레이에서 약 10km(6.2마일) 이내에 있어야 합니다.

a|
통신 방법
a|
표준 IP 또는 Fibre Channel 네트워크
a|
Fibre Channel 네트워크만 해당.

```
 a|
볼륨 유형
 a|
표준 또는 얇은.
 a|
표준 전용.

|===



[[ID633aff6625631d7bd5eb88ef9cae1595]]
= 미러링 구성 워크플로우
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Unified Manager에서 비동기식 또는 동기식 미러링을 구성한 다음 System Manager를
사용하여 동기화를 관리합니다.



== 비동기식 미러링 워크플로우

비동기식 미러링에는 다음 워크플로우가 포함됩니다.

. Unified Manager에서 초기 구성을 수행합니다.
+
.. 로컬 스토리지 배열을 데이터 전송 소스로 선택합니다.
.. 로컬 스토리지의 운영 볼륨과 원격 스토리지의 보조 볼륨을 위한 컨테이너인 기존 미러 정합성
보장 그룹을 생성하거나 선택합니다. 운영 볼륨과 보조 볼륨을 "미러링된 페어"라고 합니다. 미러
정합성 보장 그룹을 처음으로 생성하는 경우 수동 동기화 또는 예약된 동기화를 수행할지 여부를
지정합니다.
.. 로컬 스토리지 어레이에서 운영 볼륨을 선택한 다음 예약된 용량을 확인합니다. 예약된 용량은
복제 작업에 사용할 물리적 할당 용량입니다.
.. 원격 스토리지 시스템을 전송 대상, 보조 볼륨으로 선택한 다음 예약된 용량을 결정합니다.
.. 운영 볼륨에서 보조 볼륨으로 초기 데이터 전송을 시작합니다. 볼륨 크기에 따라 이 초기
전송에 몇 시간이 걸릴 수 있습니다.


. 초기 동기화 진행률을 확인합니다.
+
```

.. Unified Manager에서 로컬 어레이에 대한 System Manager를 시작합니다.
.. System Manager에서 미러링 작업의 상태를 봅니다. 미러링이 완료되면 미러링된 쌍의 상태가 "Optimal(최적)"입니다.

. 선택적으로 System Manager에서 후속 데이터 전송을 다시 예약하거나 수동으로 수행할 수 있습니다. 운영 볼륨에서 2차 볼륨으로 새 블록과 변경된 블록만 전송합니다.
+
[NOTE]
====
비동기식 복제는 정기적으로 수행되므로 시스템에서 변경된 블록을 통합하고 네트워크 대역폭을 보존할 수 있습니다. 쓰기 처리량과 쓰기 지연 시간에 미치는 영향은 미미합니다.

====

== 동기 미러링 워크플로우

동기식 미러링에는 다음 워크플로우가 포함됩니다.

. Unified Manager에서 초기 구성을 수행합니다.
+
.. 데이터 전송을 위한 소스로 로컬 스토리지 배열을 선택합니다.
.. 로컬 스토리지 어레이에서 운영 볼륨을 선택합니다.
.. 데이터 전송 대상으로 원격 스토리지 시스템을 선택한 다음 보조 볼륨을 선택합니다.
.. 동기화 및 재동기화 우선 순위를 선택합니다.
.. 운영 볼륨에서 보조 볼륨으로 초기 데이터 전송을 시작합니다. 볼륨 크기에 따라 이 초기 전송에 몇 시간이 걸릴 수 있습니다.

. 초기 동기화 진행률을 확인합니다.
+
.. Unified Manager에서 로컬 어레이에 대한 System Manager를 시작합니다.
.. System Manager에서 미러링 작업의 상태를 봅니다. 미러링이 완료되면 미러링된 쌍의 상태가 "Optimal(최적)"입니다. 두 배열은 정상적인 작업을 통해 동기화 상태를 유지하려고 합니다. 운영 볼륨에서 2차 볼륨으로 새 블록과 변경된 블록만 전송합니다.

. 선택적으로 System Manager에서 동기화 설정을 변경할 수 있습니다.
+
[NOTE]
====
동기식 복제는 지속적이기 때문에 두 사이트 간의 복제 링크는 충분한 대역폭 기능을 제공해야 합니다.

```
====



[[IDc7bc6ab14d5966e748510813ec00e389]]
= 미러링 용어
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
미러링 조건이 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

[cols="25h,~"]
|===
| 기간 | 설명


 a|
로컬 스토리지 시스템입니다
 a|
로컬 스토리지 배열은 사용자가 수행하는 스토리지 배열입니다.




 a|
미러 정합성 보장 그룹
 a|
미러 정합성 보장 그룹은 하나 이상의 미러링된 쌍에 대한 컨테이너입니다. 비동기식 미러링 작업의 경우 미러 정합성 보장 그룹을 생성해야 합니다. 그룹의 모든 미러링된 쌍이 동시에 재동기화되므로 일관된 복구 지점이 유지됩니다.

동기식 미러링은 미러 정합성 보장 그룹을 사용하지 않습니다.



 a|
미러링 쌍
 a|
미러링된 쌍은 기본 볼륨 및 보조 볼륨이라는 두 개의 볼륨으로 구성됩니다.

비동기식 미러링에서는 미러링된 쌍이 항상 미러 정합성 보장 그룹에 속합니다. 쓰기 작업은 먼저 운영 볼륨에 대해 수행된 다음 보조 볼륨에 복제됩니다. 미러 정합성 보장 그룹의 미러링된 각 쌍은 동일한 동기화 설정을 공유합니다.
```

a|
운영 볼륨
a|
미러링된 쌍의 기본 볼륨은 미러링될 소스 볼륨입니다.

a|
원격 스토리지 시스템
a|
원격 스토리지 시스템은 일반적으로 미러링 구성의 데이터 복제본을 보관하는 보조 사이트로 지정됩니다.

a|
예약된 용량입니다
a|
예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.

이러한 볼륨은 컨트롤러가 운영 상태에서 미러링을 유지하는 데 필요한 정보를 지속적으로 저장할 수 있도록 하기 위해 필요합니다. 여기에는 델타 로그 및 쓰기 시 복사 데이터와 같은 정보가 포함됩니다.

a|
2차 볼륨
a|
미러링된 쌍의 보조 볼륨은 일반적으로 보조 사이트에 위치하며 데이터 복제본을 보관합니다.

a|
동기화
a|
동기화는 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화에서 수행됩니다. 동기화는 통신 중단 후 운영 볼륨과 2차 볼륨의 동기화가 중단된 경우에도 발생합니다. 통신 링크가 다시 작동되면 복제되지 않은 모든 데이터가 보조 볼륨의 스토리지 시스템에 동기화됩니다.

|===

```
[[IDa2495362cba7057ea5b38cf12b64c701]]
= 미러링 사용에 대한 요구사항
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
미러링을 구성하려는 경우 다음 요구사항을 염두에 두십시오.



== Unified Manager를 참조하십시오

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.



== 지원합니다

[NOTE]
====
동기식 미러링은 EF600 또는 EF300 스토리지 어레이에서 사용할 수 없습니다.

====
* 두 개의 스토리지 어레이가 있어야 합니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
* 비동기 미러링은 FC(파이버 채널) 또는 iSCSI 호스트 포트가 있는 컨트롤러에서 지원되며, 동기식 미러링은 FC 호스트 포트가 있는 컨트롤러에서만 지원됩니다.
```

== 연결 요구 사항

FC 인터페이스(비동기식 또는 동기식)를 통해 미러링하려면 다음이 필요합니다.

* 스토리지 어레이의 각 컨트롤러는 가장 높은 번호가 지정된 FC 호스트 포트를 미러링 작업에 사용합니다.
* 컨트롤러에 기본 FC 포트와 HIC(호스트 인터페이스 카드) FC 포트가 모두 있는 경우 가장 높은 번호가 지정된 포트가 HIC에 있습니다. 전용 포트에 로그온한 호스트는 로그아웃되며 호스트 로그인 요청은 허용되지 않습니다. 이 포트의 I/O 요청은 미러링 작업에 사용되는 컨트롤러에서만 허용됩니다.
* 전용 미러링 포트는 디렉토리 서비스 및 네임 서비스 인터페이스를 지원하는 FC 패브릭 환경에 연결해야 합니다. 특히 FC-AL 및 지점 간 연결 옵션은 미러 관계에 참여하는 컨트롤러 간의 연결 옵션으로 지원되지 않습니다.

iSCSI 인터페이스를 통한 미러링(비동기식만 해당)에는 다음이 필요합니다.

* FC와 달리 iSCSI에는 전용 포트가 필요하지 않습니다. iSCSI 환경에서 비동기 미러링을 사용하는 경우 비동기 미러링에 사용하기 위해 스토리지 어레이의 프런트 엔드 iSCSI 포트 중 하나를 전용으로 지정할 필요가 없습니다. 이러한 포트는 비동기 미러 트래픽과 호스트-스토리지 I/O 연결을 위해 모두 공유됩니다.
* 컨트롤러는 iSCSI 이니시에이터가 세션을 설정하려고 시도하는 원격 스토리지 시스템의 목록을 유지합니다. iSCSI 연결을 성공적으로 설정하는 첫 번째 포트는 해당 원격 스토리지 시스템과의 이후의 모든 통신에 사용됩니다. 통신이 실패하면 사용 가능한 모든 포트를 사용하여 새 세션이 시도됩니다.
* iSCSI 포트는 포트별로 어레이 레벨에서 구성됩니다. 구성 메시징 및 데이터 전송을 위한 컨트롤러 간 통신은 다음 설정을 포함한 글로벌 설정을 사용합니다.
+
** VLAN: 로컬 시스템과 원격 시스템 모두 동일한 VLAN 설정을 사용하여 통신해야 합니다
** iSCSI 수신 포트입니다
** 점보 프레임
** 이더넷 우선 순위

[NOTE]
====
iSCSI 인터컨트롤러 통신은 관리 이더넷 포트가 아닌 호스트 연결 포트를 사용해야 합니다.

====

== 미러링 볼륨 후보

* RAID 레벨, 캐싱 매개 변수 및 세그먼트 크기는 미러링된 쌍의 운영 볼륨과 2차 볼륨에서 서로

다를 수 있습니다.
+

NOTE: EF600 및 EF300 컨트롤러의 경우 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨이 동일한 프로토콜, 트레이 레벨, 세그먼트 크기, 보안 유형 및 RAID 레벨과 일치해야 합니다. 사용 가능한 볼륨 목록에 비적격한 비동기 미러링 쌍이 나타나지 않습니다.

* 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.
* 볼륨은 하나의 미러 관계에만 참여할 수 있습니다.
* 동기식 미러링 쌍의 경우 운영 볼륨과 2차 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨 또는 스냅샷 볼륨일 수 없습니다.
* 동기식 미러링의 경우 지정된 스토리지 어레이에서 지원되는 볼륨 수에 제한이 있습니다. 스토리지 배열에 구성된 볼륨 수가 지원되는 제한보다 적었는지 확인합니다. 동기식 미러링이 활성 상태인 경우 생성된 2개의 예약된 용량 볼륨이 볼륨 제한에 대해 계산됩니다.
* 비동기식 미러링의 경우 운영 볼륨과 2차 볼륨의 드라이브 보안 기능이 동일해야 합니다.
+
** 기본 볼륨이 FIPS를 지원할 수 있는 경우 보조 볼륨은 FIPS를 지원할 수 있어야 합니다.
** 기본 볼륨이 FDE를 지원할 수 있는 경우 보조 볼륨은 FDE를 지원할 수 있어야 합니다.
** 주 볼륨이 드라이브 보안을 사용하지 않는 경우 보조 볼륨이 드라이브 보안을 사용하지 않아야 합니다.

== 예약된 용량입니다

비동기식 미러링:

* 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위해 쓰기 정보를 로깅하기 위해 미러링된 쌍의 보조 볼륨과 운영 볼륨에 예약된 용량 볼륨이 필요합니다.
* 미러링 쌍의 운영 볼륨과 2차 볼륨 모두에 추가 예약 용량이 필요하므로 미러 관계의 두 스토리지 어레이에서 사용 가능한 용량이 있는지 확인해야 합니다.

동기식 미러링:

* 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위해 쓰기 정보를 로깅하기 위해 운영 볼륨과 보조 볼륨에 예약된 용량이 필요합니다.
* 예약된 용량 볼륨은 동기식 미러링이 활성화될 때 자동으로 생성됩니다. 미러링된 쌍의 운영 볼륨과 2차 볼륨 모두에 예약된 용량이 필요하므로 동기 미러 관계에 참여하는 두 스토리지 시스템에서 사용 가능한 용량이 충분한지 확인해야 합니다.

== 드라이브 보안 기능

* 보안 가능 드라이브를 사용하는 경우 기본 볼륨 및 보조 볼륨에 호환되는 보안 설정이 있어야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
* 보안 가능 드라이브를 사용하는 경우 기본 볼륨과 보조 볼륨은 동일한 드라이브 유형을 사용해야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
* DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.

:leveloffset: -1

= 미러링을 구성합니다

:leveloffset: +1

[[IDd13aaf4478b5d1e232c37a9ccca8e40e]]
= 비동기 미러링 쌍을 생성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
비동기식 미러링을 구성하려면 로컬 스토리지의 기본 볼륨과 원격 스토리지의 보조 볼륨을 포함하는 미러링된 쌍을 생성합니다.

.시작하기 전에
미러링된 쌍을 생성하기 전에 Unified Manager에 대한 다음 요구사항을 충족해야 합니다.

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.

또한 스토리지 어레이 및 볼륨에 대한 다음 요구 사항도 충족해야 합니다.

* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며

네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
* 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.
* 비동기식 미러 관계에 사용할 운영 볼륨과 2차 볼륨을 모두 생성했습니다.
* 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.

.이 작업에 대해
비동기 미러링 쌍을 만드는 프로세스는 다단계 절차입니다.

== 1단계: 미러 정합성 보장 그룹을 생성하거나 선택합니다

이 단계에서는 새 미러 일관성 그룹을 생성하거나 기존 미러 일관성 그룹을 선택합니다. 미러 정합성 보장 그룹은 운영 볼륨과 2차 볼륨(미러링된 페어)의 컨테이너로, 그룹의 모든 페어에 대해 원하는 재동기화 방법(수동 또는 자동)을 지정합니다.

.단계
. Manage * 페이지에서 소스에 사용할 로컬 스토리지 배열을 선택합니다.
. 메뉴 선택: 작업 [비동기 미러링 쌍 만들기].
+
Create Asynchronous Mirrored Pair 마법사가 열립니다.

. 기존 미러 정합성 보장 그룹을 선택하거나 새 미러 정합성 보장 그룹을 생성합니다.
+
기존 그룹을 선택하려면 * 기존 미러 정합성 보장 그룹 * 이 선택되어 있는지 확인한 다음 테이블에서 그룹을 선택합니다. 일관성 그룹에는 여러 개의 미러링된 쌍이 포함될 수 있습니다.

+
새 그룹을 만들려면 다음을 수행합니다.

+
.. 새 미러 정합성 보장 그룹 * 을 선택한 후 * 다음 * 을 클릭합니다.
.. 두 스토리지 배열 간에 미러링될 볼륨의 데이터를 가장 잘 설명하는 고유한 이름을 입력합니다. 이름은 문자, 숫자 및 밑줄(_), 대시(-) 및 해시 기호(#)로만 구성될 수 있습니다. 이름은 30자를 초과할 수 없으며 공백을 포함할 수 없습니다.
.. 로컬 스토리지 시스템과 미러 관계를 설정할 원격 스토리지 시스템을 선택합니다.
+
[NOTE]
====
원격 스토리지 배열이 암호로 보호되어 있는 경우 암호를 입력하라는 메시지가 표시됩니다.

====
.. 미러링된 쌍을 수동으로 동기화할지 또는 자동으로 동기화할지 여부를 선택합니다.
+
*** * 수동 * -- 이 그룹 내에서 미러링된 모든 쌍의 동기화를 수동으로 시작하려면 이 옵션을 선택합니다. 나중에 재동기화를 수행하려면 운영 스토리지 시스템에 대해 System Manager를 시작한 다음 메뉴(Storage [Asynchronous Mirroring])로 이동하여 * Mirror Consistency Groups * 탭에서 그룹을 선택한 다음 menu: More [Manually resyncize]를 선택합니다.
*** * 자동 * - 이전 업데이트 시작에서 다음 업데이트 시작까지 원하는 간격을 * 분 *, * 시간 * 또는 * 일 * 으로 선택합니다. 예를 들어 동기화 간격이 30분으로 설정되어 있고 동기화 프로세스가 오후 4시에 시작되면 다음 프로세스는 오후 4시 30분에 시작됩니다


.. 원하는 알림 설정을 선택합니다.
+
*** 수동 동기화의 경우 알림을 받을 때의 임계값(남은 용량 백분율로 정의)을 지정합니다.
*** 자동 동기화의 경우 세 가지 알림 방법을 설정할 수 있습니다. 특정 시간 동안 동기화가 완료되지 않은 경우, 원격 스토리지의 복구 지점 데이터가 특정 시간 제한보다 오래되고 예약된 용량이 특정 임계값(남은 용량 백분율로 정의)에 근접하는 경우




. 다음 * 을 선택하고 로 이동합니다<<2단계: 운영 볼륨을 선택합니다>>.
+
새 미러 정합성 보장 그룹을 정의한 경우 Unified Manager는 먼저 로컬 스토리지 시스템에 미러 정합성 보장 그룹을 생성한 다음 원격 스토리지 시스템에 미러 정합성 보장 그룹을 생성합니다. 각 어레이에 대해 System Manager를 시작하여 미러 정합성 보장 그룹을 보고 관리할 수 있습니다.

+
[NOTE]
====
Unified Manager가 로컬 스토리지 시스템에 미러 정합성 보장 그룹을 생성했지만 원격 스토리지 시스템에 생성하지 못한 경우 로컬 스토리지 시스템에서 미러 정합성 보장 그룹이 자동으로 삭제됩니다. Unified Manager에서 미러 정합성 보장 그룹을 삭제하려는 동안 오류가 발생하면 수동으로 삭제해야 합니다.

====




== 2단계: 운영 볼륨을 선택합니다

이 단계에서는 미러 관계에 사용할 운영 볼륨을 선택하고 예약된 용량을 할당합니다. 로컬 스토리지 배열에서 운영 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다.

로컬 스토리지 시스템의 미러 정합성 보장 그룹에 추가하는 모든 볼륨은 미러 관계에서 기본 역할을 유지합니다.

.단계
. 사용 가능한 볼륨 목록에서 운영 볼륨으로 사용할 볼륨을 선택한 후 * Next * 를 클릭하여 예약된 용량을 할당합니다.
. 적합한 후보 목록에서 운영 볼륨에 대해 예약된 용량을 선택합니다.
+
다음 지침을 염두에 두십시오.

+
** 예약된 용량의 기본 설정은 기본 볼륨 용량의 20%이며 일반적으로 이 용량이면 충분합니다. 비율을 변경한 경우 * 후보 새로 고침 * 을 클릭합니다.
** 필요한 용량은 운영 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 용량을 유지하는 데 필요한 기간에 따라 달라집니다.
** 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 용량을 선택합니다.
+
*** 미러링 쌍을 장기간 유지하려고 합니다.
*** 입출력 작업이 많은 경우 운영 볼륨에서 데이터 블록의 비율이 크게 변경됩니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

. 다음 * 을 선택하고 로 이동합니다<<3단계: 보조 볼륨을 선택합니다>>.

== 3단계: 보조 볼륨을 선택합니다

이 단계에서는 미러 관계에 사용할 보조 볼륨을 선택하고 예약된 용량을 할당합니다. 원격 스토리지 어레이에서 보조 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다.

원격 스토리지 시스템의 미러 정합성 보장 그룹에 추가하는 모든 볼륨은 미러 관계에서 2차 역할을 유지합니다.

.단계
. 적합한 볼륨 목록에서 미러링된 쌍의 보조 볼륨으로 사용할 볼륨을 선택한 후 * Next * 를 클릭하여 예약된 용량을 할당합니다.
. 적합한 후보 목록에서 2차 볼륨에 대해 예약된 용량을 선택합니다.
+
다음 지침을 염두에 두십시오.

+
** 예약된 용량의 기본 설정은 기본 볼륨 용량의 20%이며 일반적으로 이 용량이면 충분합니다. 비율을 변경한 경우 * 후보 새로 고침 * 을 클릭합니다.
** 필요한 용량은 운영 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 용량을 유지하는 데 필요한 기간에 따라 달라집니다.
** 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 용량을 선택합니다.
+
*** 미러링 쌍을 장기간 유지하려고 합니다.
*** 입출력 작업이 많은 경우 운영 볼륨에서 데이터 블록의 비율이 크게 변경됩니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

. 비동기 미러링 시퀀스를 완료하려면 * Finish * 를 선택합니다.

.결과
Unified Manager는 다음 작업을 수행합니다.

* 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화를 시작합니다.
* 로컬 스토리지 시스템 및 원격 스토리지 시스템에서 미러링된 쌍에 대한 예약된 용량을 생성합니다.

NOTE: 미러링되는 볼륨이 씬 볼륨인 경우 초기 동기화 중에 프로비저닝된 블록(보고된 용량이 아닌 할당된 용량)만 보조 볼륨으로 전송됩니다. 이렇게 하면 초기 동기화를 완료하기 위해 전송해야 하는 데이터의 양이 줄어듭니다.

[[ID807cd7611a5e8eafc53fe7f8ce9af70a]]
= 동기식 미러링 쌍을 생성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
동기식 미러링을 구성하려면 로컬 스토리지의 기본 볼륨과 원격 스토리지의 보조 볼륨을 포함하는 미러링된 쌍을 생성합니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

====
.시작하기 전에
미러링된 쌍을 생성하기 전에 Unified Manager에 대한 다음 요구사항을 충족해야 합니다.

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.

또한 스토리지 어레이 및 볼륨에 대한 다음 요구 사항도 충족해야 합니다.

* 미러링에 사용할 두 스토리지 어레이가 Unified Manager에서 검색됩니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭을 통해 연결됩니다.
* 동기식 미러 관계에 사용할 운영 볼륨과 2차 볼륨을 모두 생성했습니다.
* 운영 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨이거나 스냅샷 볼륨일 수 없습니다.
* 2차 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨이거나 스냅샷 볼륨일 수 없습니다.
* 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.

.이 작업에 대해
동기식 미러링 쌍을 생성하는 프로세스는 여러 단계로 이루어집니다.

== 1단계: 운영 볼륨을 선택합니다

이 단계에서는 동기식 미러 관계에 사용할 운영 볼륨을 선택합니다. 로컬 스토리지 배열에서 운영 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 선택한 볼륨은 미러 관계에서 1차 역할을 보유합니다.

.단계
. Manage * 페이지에서 소스에 사용할 로컬 스토리지 배열을 선택합니다.
. 메뉴 선택: 작업 [동기식 미러링 쌍 생성].
+
동기식 미러링 쌍 생성 마법사가 열립니다.

. 적합한 볼륨 목록에서 미러의 운영 볼륨으로 사용할 볼륨을 선택합니다.
. 다음 * 을 선택하고 로 이동합니다<<2단계: 보조 볼륨을 선택합니다>>.

== 2단계: 보조 볼륨을 선택합니다

이 단계에서는 미러 관계에 사용할 보조 볼륨을 선택합니다. 원격 스토리지 어레이에서 보조 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 선택한 볼륨은 미러 관계에서 2차 역할을 유지합니다.

.단계
. 로컬 스토리지 시스템과 미러 관계를 설정할 원격 스토리지 시스템을 선택합니다.
+
[NOTE]
====
원격 스토리지 배열이 암호로 보호되어 있는 경우 암호를 입력하라는 메시지가 표시됩니다.

====
+
** 스토리지 배열은 해당 스토리지 배열 이름으로 나열됩니다. 스토리지 배열의 이름을 지정하지 않은 경우 이름이 "UNNAMED(명명되지 않음)"으로 표시됩니다.
** 사용하려는 스토리지 어레이가 목록에 없는 경우 Unified Manager에서 검색된 스토리지인지 확인합니다.

. 적합한 볼륨 목록에서 미러의 2차 볼륨으로 사용할 볼륨을 선택합니다.
+
[NOTE]
====
운영 볼륨보다 큰 용량으로 2차 볼륨을 선택하는 경우 사용 가능한 용량이 운영 볼륨의 크기로 제한됩니다.

====
. 다음 * 을 클릭하고 로 이동합니다<<3단계: 동기화 설정을 선택합니다>>.

== 3단계: 동기화 설정을 선택합니다

이 단계에서는 통신 중단 후 데이터 동기화 방법을 결정하는 설정을 선택합니다. 통신이 중단된 후 기본 볼륨의 컨트롤러 소유자가 데이터를 보조 볼륨과 재동기화하는 우선 순위를 설정할 수 있습니다. 수동 또는 자동 재동기화 정책도 선택해야 합니다.

.단계
. 슬라이더 막대를 사용하여 동기화 우선 순위를 설정합니다.
+
동기화 우선 순위는 서비스 입출력 요청과 비교하여 통신 중단 후 초기 동기화 및 재동기화 작업을 완료하는 데 사용되는 시스템 리소스의 양을 결정합니다.

+
이 대화 상자에 설정된 우선 순위는 운영 볼륨과 2차 볼륨 모두에 적용됩니다. 나중에 System Manager로 이동하여 메뉴에서 스토리지 [동기식 미러링 > 자세히 > 설정 편집]을 선택하여 기본 볼륨의 속도를 수정할 수 있습니다.

+
동기화 우선 순위는 5가지입니다.

+
** 최저
** 낮음
** 중간
** 높음
** 최고
+
동기화 우선 순위가 가장 낮은 속도로 설정된 경우 입출력 작업의 우선 순위가 지정되고 재동기화 작업이 더 오래 걸립니다. 동기화 우선 순위가 가장 높은 속도로 설정된 경우 재동기화 작업의 우선 순위가 지정되지만 스토리지 시스템의 입출력 작업이 영향을 받을 수 있습니다.

. 원격 스토리지 시스템에서 미러링된 쌍을 수동 또는 자동으로 재동기화할지 여부를 선택합니다.
+
** * 수동 * (권장 옵션) -- 미러링된 쌍으로 통신이 복구된 후 수동으로 동기화를 재개하려면 이 옵션을 선택합니다. 이 옵션은 데이터를 복구할 수 있는 최적의 기회를 제공합니다.
** * 자동 * -- 통신이 미러링된 쌍으로 복구된 후 재동기화를 자동으로 시작하려면 이 옵션을 선택합니다.
+
동기화를 수동으로 재개하려면 System Manager로 이동하여 메뉴에서 Storage [Synchronous Mirroring](저장소 [Synchronous Mirroring])을 선택하고 표에서 미러링된 쌍을 강조 표시한 다음 * More *(기타 *) * 에서 * Resume * 을 선택합니다.

. 동기식 미러링 시퀀스를 완료하려면 * Finish * 를 클릭합니다.

.결과
미러링이 활성화되면 시스템은 다음 작업을 수행합니다.

* 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화를 시작합니다.

* 동기화 우선 순위 및 재동기화 정책을 설정합니다.
* 미러 데이터 전송을 위해 컨트롤러 HIC에서 가장 높은 번호의 포트를 예약합니다.
+
이 포트에서 수신된 I/O 요청은 미러링된 쌍에 있는 보조 볼륨의 원격 기본 컨트롤러 소유자만이 허용됩니다. (기본 볼륨에 대한 예약이 허용됩니다.)

* 각 컨트롤러에 대해 하나씩, 예약된 용량 볼륨 2개를 생성합니다. 이 볼륨은 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위한 쓰기 정보를 로깅하는 데 사용됩니다.
+
각 볼륨의 용량은 128MiB입니다. 하지만 볼륨이 풀에 배치되면 4GiB가 각 볼륨에 대해 예약됩니다.

.작업을 마친 후
System Manager로 이동하여 Home [View Operations in Progress] 메뉴를 선택하여 동기 미러링 작업의 진행률을 확인합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

:leveloffset: -1

= FAQ 를 참조하십시오

:leveloffset: +1

[[IDb2736375fcc0f240cce5b8fb959b69e5]]
= 미러 정합성 보장 그룹을 생성하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
미러 일관성 그룹을 생성하기 전에 다음 지침을 따르십시오.

Unified Manager에 대한 다음 요구사항을 충족합니다.

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로

이동하여 자체 보안 인증서를 설치할 수 있습니다.

또한 스토리지 어레이에 대한 다음 요구 사항도 충족해야 합니다.

* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====

[[IDbe94af11cda35c479939dc4f0b7e382a]]
= 미러링된 쌍을 만들기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
대칭 복사된 쌍을 만들기 전에 다음 지침을 따릅니다.

* 두 개의 스토리지 어레이가 있어야 합니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
* 비동기 미러링은 FC(파이버 채널) 또는 iSCSI 호스트 포트가 있는 컨트롤러에서 지원되며, 동기식 미러링은 FC 호스트 포트가 있는 컨트롤러에서만 지원됩니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====

[[ID44c2da6655708451ffe9ea610753574c]]
= 이 비율을 변경하는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
일반적으로 예약된 용량은 비동기식 미러링 작업을 위한 기본 볼륨의 20%입니다. 일반적으로 이 용량이면 충분합니다.

필요한 용량은 기본 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 스토리지 오브젝트의 복사 서비스 작업을 사용할 기간에 따라 달라집니다. 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 비율을 선택합니다.

* 특정 스토리지 오브젝트의 복사 서비스 작업 수명이 매우 긴 경우
* 입출력 작업이 많은 경우 기본 볼륨에서 데이터 블록의 비율이 크게 변경될 수 있습니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

[[ID45a0ce7298c5d1a26c86cac27120570c]]
= 예약된 용량이 두 개 이상 표시되는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
풀 또는 볼륨 그룹에 스토리지 객체에 대해 선택한 용량 비율을 충족하는 볼륨이 두 개 이상 있는 경우 여러 후보가 표시됩니다.

복사 서비스 작업을 위해 기본 볼륨에 예약할 물리적 드라이브 공간의 비율을 변경하여 권장되는 후보 목록을 새로 고칠 수 있습니다. 선택한 내용에 따라 가장 적합한 후보가 표시됩니다.

[[IDc89bd6e596aebd24172b19ad383c38b8]]
= 내 볼륨이 모두 표시되지 않는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
미러링된 쌍의 기본 볼륨을 선택하면 목록에 모든 적격 볼륨이 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

* 볼륨이 최적이 아닙니다.
* 볼륨이 이미 미러링 관계에 있습니다.
* 동기식 미러링의 경우 미러링된 쌍의 운영 볼륨과 2차 볼륨이 표준 볼륨이어야 합니다. 씬 볼륨 또는 스냅샷 볼륨일 수 없습니다.
* 비동기식 미러링의 경우 씬 볼륨에 자동 확장이 설정되어 있어야 합니다.

NOTE: EF600 및 EF300 컨트롤러의 경우 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨이 동일한 프로토콜, 트레이 레벨, 세그먼트 크기, 보안 유형 및 RAID 레벨과 일치해야 합니다. 사용 가능한 볼륨 목록에 비적격한 비동기 미러링 쌍이 나타나지 않습니다.

[[IDfba6dc4474034799d5f2228836a8ebbe]]
= 원격 스토리지 어레이에 볼륨이 모두 표시되지 않는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
원격 스토리지 어레이에서 보조 볼륨을 선택할 경우 목록에 해당 미러링된 쌍에 대해 적합한 볼륨이 모두 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

* 볼륨은 스냅샷 볼륨과 같이 비표준 볼륨입니다.
* 볼륨이 최적이 아닙니다.

* 볼륨이 이미 미러링 관계에 있습니다.
* 비동기식 미러링의 경우 운영 볼륨과 2차 볼륨 간의 씬 볼륨 특성이 일치하지 않습니다.
* DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.
+
** 운영 볼륨이 DA를 사용하는 경우 보조 볼륨은 DA를 활성화해야 합니다.
** 운영 볼륨이 DA를 사용하지 않는 경우 보조 볼륨을 DA로 설정하지 않아야 합니다.

* 비동기식 미러링의 경우 운영 볼륨과 2차 볼륨의 드라이브 보안 기능이 동일해야 합니다.
+
** 기본 볼륨이 FIPS를 지원할 수 있는 경우 보조 볼륨은 FIPS를 지원할 수 있어야 합니다.
** 기본 볼륨이 FDE를 지원할 수 있는 경우 보조 볼륨은 FDE를 지원할 수 있어야 합니다.
** 주 볼륨이 드라이브 보안을 사용하지 않는 경우 보조 볼륨이 드라이브 보안을 사용하지 않아야 합니다.

[[ID7107a79a741acee9999010ecc0d856a1]]
= 동기화 우선 순위가 동기화 속도에 어떤 영향을 미칩니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
동기화 우선 순위는 시스템 성능과 관련하여 동기화 작업에 할당되는 처리 시간을 정의합니다.

운영 볼륨의 컨트롤러 소유자가 이 작업을 백그라운드에서 수행합니다. 동시에 컨트롤러 소유자가 운영 볼륨에 대한 로컬 I/O 쓰기 및 보조 볼륨에 대한 관련 원격 쓰기를 처리합니다. 재동기화는 컨트롤러 처리 리소스를 입출력 작업에서 전환하므로 재동기화는 호스트 애플리케이션의 성능에 영향을 미칠 수 있습니다.

동기화 우선 순위가 얼마나 오래 걸릴 수 있고 동기화 우선 순위가 시스템 성능에 어떤 영향을 미칠 수 있는지 결정할 수 있도록 이 지침을 염두에 두십시오.

다음과 같은 우선 순위가 있습니다.

* 최저
* 낮음
* 중간
* 높음
* 최고

우선 순위가 가장 낮은 속도는 시스템 성능을 지원하지만 재동기화에 더 많은 시간이 걸립니다. 우선 순위가 가장 높은 속도가 재동기화를 지원하지만 시스템 성능이 저하될 수 있습니다.

이 지침은 우선 순위 간의 차이를 대략적으로 나타냅니다.

[cols="45h,~"]
|===
| 전체 동기화의 우선 순위 속도 | 최고 동기화 속도에 비해 경과된 시간입니다

a|
최저
a|
최고 우선 순위인 경우 약 8배

a|
낮음
a|
최고 우선 순위인 경우 약 6배

a|
중간
a|
가장 높은 우선 순위에서 약 3배 반 정도 소요됩니다.

a|
높음
a|
최고 우선 순위보다 약 2배 긴 시간.

|===
볼륨 크기 및 호스트 I/O 속도 로드는 동기화 시간 비교에 영향을 줍니다.

[[IDee21753297da689e94eed24fc14d2b3a]]
= 수동 동기화 정책을 사용하는 것이 권장되는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
수동 재동기화는 재동기화 프로세스를 관리하여 데이터를 복구할 수 있는 최적의 기회를 제공하기 때문에 권장됩니다.

자동 재동기화 정책을 사용하고 재동기화 중에 간헐적인 통신 문제가 발생하는 경우 보조 볼륨의 데이터가 일시적으로 손상될 수 있습니다. 재동기화가 완료되면 데이터가 수정됩니다.



:leveloffset: -1


:leveloffset: -1


= 인증서

:leveloffset: +1


[[IDebcb9e423ba32f7e058df2d4807bb76a]]
= 인증서 개요
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증서 관리를 사용하면 CSR(인증서 서명 요청)을 생성하고 인증서를 가져오고 기존 인증서를 관리할 수 있습니다.



== 인증서란 무엇입니까?

_Certificates_는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다. 인증서 유형에는 두 가지가 있습니다. CA(인증 기관)에서 _signed certificate_를 검증하고, 타사 대신 엔터티의 소유자가 _self-signed certificate_를 확인합니다.

자세한 내용:

* xref:{relative_path}how-certificates-work-unified.html["인증서 작동 방식"]
```

```
* xref:{relative_path}certificate-terminology-unified.html["인증서 용어"]



== 인증서를 구성하려면 어떻게 합니까?

인증서 관리에서 Unified Manager를 호스팅하는 관리 스테이션에 대한 인증서를 구성하고
스토리지 시스템의 컨트롤러에 대한 인증서를 가져올 수 있습니다.

자세한 내용:

* xref:{relative_path}use-ca-signed-certificate-um.html["관리 시스템에 CA 서명
인증서를 사용합니다"]
* xref:{relative_path}import-array-certificates-unified.html["스토리지에 대한
인증서를 가져옵니다"]



= 개념

:leveloffset: +1


[[IDb2e6cf015dd58378427c1bb5b011488d]]
= 인증서 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증서는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털
파일입니다.



== 서명된 인증서

인증서는 웹 통신이 지정된 서버와 클라이언트 사이에서만 암호화된 형식으로 비공개로, 변경되지
않도록 합니다. Unified Manager를 사용하면 호스트 관리 시스템의 브라우저 인증서와 검색된
스토리지 시스템의 컨트롤러를 관리할 수 있습니다.

인증서는 신뢰할 수 있는 기관에서 서명할 수도 있고 자체 서명할 수도 있습니다. "서명"은 단순히
누군가가 소유자의 신원을 확인하고 자신의 장치를 신뢰할 수 있다는 것을 확인하는 것을
```

의미합니다. 스토리지 어레이에는 각 컨트롤러에서 자동으로 생성된 자체 서명 인증서가 함께 제공됩니다. 자체 서명된 인증서를 계속 사용하거나 컨트롤러와 호스트 시스템 간의 보다 안전한 연결을 위해 CA 서명 인증서를 얻을 수 있습니다.

[NOTE]
====
CA 서명 인증서는 향상된 보안 보호 기능을 제공하지만(예: 중간의 공격 방지) 대규모 네트워크를 사용하는 경우 비용이 많이 들 수 있습니다. 반면 자체 서명된 인증서는 보안성이 떨어지지만 무료입니다. 따라서 자체 서명된 인증서는 프로덕션 환경이 아닌 내부 테스트 환경에 가장 많이 사용됩니다.

====
서명된 인증서는 신뢰할 수 있는 타사 조직인 CA(인증 기관)에서 유효성을 검사합니다. 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보, 인증서 발급 및 만료 날짜, 엔터티에 대한 유효한 도메인 및 문자와 숫자로 구성된 디지털 서명이 포함됩니다.

브라우저를 열고 웹 주소를 입력하면 시스템은 백그라운드에서 인증서 확인 프로세스를 수행하여 유효한 CA 서명 인증서가 포함된 웹 사이트에 연결 중인지 확인합니다. 일반적으로 서명된 인증서로 보호되는 사이트에는 자물쇠 아이콘과 주소에 https 지정이 포함되어 있습니다. CA 서명 인증서가 없는 웹 사이트에 연결하려고 하면 브라우저에 사이트가 안전하지 않음을 알리는 경고가 표시됩니다.

CA는 응용 프로그램 프로세스 중에 ID를 확인하는 단계를 수행합니다. 등록된 회사에 이메일을 보내고, 회사 주소를 확인하고, HTTP 또는 DNS 확인을 수행할 수 있습니다. 응용 프로그램 프로세스가 완료되면 CA는 호스트 관리 시스템에 로드할 디지털 파일을 보냅니다. 일반적으로 이러한 파일에는 다음과 같은 신뢰 체인이 포함됩니다.

* * 루트 * -- 계층 구조의 맨 위에 루트 인증서가 있으며, 이 인증서에는 다른 인증서에 서명하는 데 사용되는 개인 키가 들어 있습니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.
* * 중급 * -- 루트에서 오프하는 것은 중간 인증서입니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.
* * 서버 * -- 체인 하단에 있는 서버 인증서는 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 어레이의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

== 자체 서명된 인증서

스토리지 어레이의 각 컨트롤러에는 사전 설치된 자체 서명된 인증서가 포함되어 있습니다. 자체 서명된 인증서는 타사 대신 개체 소유자가 유효성을 검사한다는 점을 제외하면 CA 서명 인증서와 비슷합니다. CA 서명 인증서와 마찬가지로 자체 서명된 인증서에는 자체 개인 키가 포함되어 있으며, 서버와 클라이언트 간의 HTTPS 연결을 통해 데이터가 암호화되고 전송되도록 합니다.

자체 서명된 인증서는 브라우저에서 "신뢰할 수 있는" 인증서가 아닙니다. 자체 서명된 인증서만 포함된 웹 사이트에 연결할 때마다 브라우저에 경고 메시지가 표시됩니다. 웹 사이트로 이동할 수

있는 경고 메시지의 링크를 클릭해야 합니다. 이렇게 하면 자체 서명된 인증서를 기본적으로 수락하게 됩니다.

== Unified Manager용 인증서

Unified Manager 인터페이스는 호스트 시스템의 웹 서비스 프록시와 함께 설치됩니다. 브라우저를 열고 Unified Manager에 연결하려고 하면 브라우저에서 디지털 인증서를 확인하여 호스트가 신뢰할 수 있는 소스인지 확인합니다. 브라우저에서 서버의 CA 서명 인증서를 찾지 못하면 경고 메시지가 열립니다. 이 페이지에서 웹 사이트로 이동하여 해당 세션에 대해 자체 서명된 인증서를 수락할 수 있습니다. 또는 CA로부터 서명된 디지털 인증서를 받을 수 있으므로 경고 메시지가 더 이상 표시되지 않습니다.

== 컨트롤러의 인증서

Unified Manager 세션 중에 CA 서명된 인증서가 없는 컨트롤러에 액세스하려고 하면 추가 보안 메시지가 표시될 수 있습니다. 이 경우 자체 서명된 인증서를 영구적으로 신뢰하거나 컨트롤러의 CA 서명 인증서를 가져올 수 있습니다. 그러면 웹 서비스 프록시 서버에서 이러한 컨트롤러의 들어오는 클라이언트 요청을 인증할 수 있습니다.

[[ID9cb0c252948e6fa70c22bafd7dd0db69]]
= 인증서 용어
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
다음 용어는 인증서 관리에 적용됩니다.

[cols="25h,~"]
|===
| 기간 | 설명

 a|
CA
 a|
CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.

a|
CSR
a|
CSR(인증서 서명 요청)은 신청자가 CA(인증 기관)로 보내는 메시지입니다. CSR은 CA가 인증서를 발급하는 데 필요한 정보를 확인합니다.

a|
인증서
a|
인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.

a|
인증서 체인
a|
인증서에 보안 계층을 추가하는 파일의 계층 구조입니다. 일반적으로 체인은 계층 맨 위에 루트 인증서 하나, 중간 인증서 하나 이상 및 엔터티를 식별하는 서버 인증서를 포함합니다.

a|
중간 인증서
a|
하나 이상의 중간 인증서가 인증서 체인의 루트에서 분기됩니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.

a|
키 저장소
a|
키 저장소는 해당 공개 키 및 인증서와 함께 개인 키가 들어 있는 호스트 관리 시스템의 리포지토리입니다. 이러한 키와 인증서는 컨트롤러와 같은 사용자 고유의 엔터티를 식별합니다.

a|
루트 인증서입니다
a|

루트 인증서는 인증서 체인의 계층 구조 맨 위에 있으며 다른 인증서에 서명하는 데 사용되는 개인 키를 포함합니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.

 a|
서명된 인증서
 a|
CA(인증 기관)에서 유효성을 검사하는 인증서입니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 또한 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보와 문자와 숫자로 구성된 디지털 서명이 포함됩니다. 서명된 인증서는 신뢰 체인을 사용하므로 프로덕션 환경에서 가장 많이 사용됩니다. "CA 서명 인증서" 또는 "관리 인증서"라고도 합니다.

 a|
자체 서명된 인증서
 a|
자체 서명된 인증서는 해당 엔터티의 소유자에 의해 유효성이 검사됩니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 문자와 숫자로 구성된 디지털 서명도 포함되어 있습니다. 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않으므로 테스트 환경에서 가장 많이 사용됩니다. "사전 설치된" 인증서라고도 합니다.

 a|
서버 인증서
 a|
서버 인증서는 인증서 체인의 맨 아래에 있습니다. 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 시스템의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

 a|
트러스토어
 a|
Truststore는 CA와 같이 신뢰할 수 있는 타사의 인증서가 포함된 저장소입니다.

|===

:leveloffset: -1

```
[[IDf3f6d7d1ffb652ff89d4992c1140db40]]
= 관리 시스템에 CA 서명 인증서를 사용합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Unified Manager를 호스팅하는 관리 시스템에 안전하게 액세스하기 위해 CA 서명 인증서를 받아서 가져올 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.이 작업에 대해
CA 서명 인증서를 사용하는 것은 3단계 절차입니다.



== 1단계: CSR 파일을 완료합니다

먼저 웹 서비스 프록시 및 Unified Manager가 설치된 조직 및 호스트 시스템을 식별하는 인증서 서명 요청(CSR) 파일을 생성해야 합니다.

[NOTE]
====
또는 OpenSSL과 같은 도구를 사용하여 CSR 파일을 생성하고 로 건너뛸 수 있습니다<<2단계: CSR 파일을 제출합니다>>.

====
.단계
. 인증서 관리 * 를 선택합니다.
. 관리 탭에서 * CSR 완료 * 를 선택합니다.
. 다음 정보를 입력하고 * 다음 * 을 클릭합니다.
+
** * 조직 * -- 회사 또는 조직의 전체 법적 이름. Inc. 또는 Corp.와 같은 접미사를 포함합니다
** * 조직 단위(선택 사항) * -- 인증서를 처리하는 조직의 사업부입니다.
** * 시/군/구 * -- 호스트 시스템이나 업무가 위치한 도시.
** * 주/지역(선택 사항) * -- 호스트 시스템 또는 비즈니스가 위치한 주 또는 지역입니다.
** * 국가 ISO 코드 * -- 미국 등 해당 국가의 2자리 ISO(International Organization for Standardization) 코드입니다.
```

. 웹 서비스 프록시가 설치된 호스트 시스템에 대한 다음 정보를 입력합니다.
+
** * 공통 이름 * -- 웹 서비스 프록시가 설치된 호스트 시스템의 IP 주소 또는 DNS 이름입니다. 주소가 올바른지 확인합니다. 입력한 주소와 정확하게 일치해야 브라우저에서 Unified Manager에 액세스할 수 있습니다. http:// 또는 https://.를 포함하지 마십시오 DNS 이름은 와일드카드로 시작할 수 없습니다.
** * 대체 IP 주소 * -- 공통 이름이 IP 주소인 경우 호스트 시스템에 대한 추가 IP 주소 또는 별칭을 선택적으로 입력할 수 있습니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다.
** * 대체 DNS 이름 * -- 공통 이름이 DNS 이름이면 호스트 시스템에 대한 추가 DNS 이름을 입력합니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다. 대체 DNS 이름이 없지만 첫 번째 필드에 DNS 이름을 입력한 경우 여기에 해당 이름을 복사합니다. DNS 이름은 와일드카드로 시작할 수 없습니다.

. 호스트 정보가 올바른지 확인합니다. 그렇지 않으면 CA에서 반환된 인증서를 가져오려고 할 때 실패합니다.
. 마침 * 을 클릭합니다.
. 로 이동합니다. <<2단계: CSR 파일을 제출합니다>>

== 2단계: CSR 파일을 제출합니다

CSR(인증서 서명 요청) 파일을 생성한 후 CA(인증 기관)로 보내 Unified Manager 및 웹 서비스 프록시를 호스팅하는 시스템에 대한 서명된 관리 인증서를 받습니다.

NOTE: E-Series 시스템에는 .pem, .crt, .cer 또는 .key 파일 형식을 포함하는 서명된 인증서에 대한 PEM 형식(Base64 ASCII 인코딩)이 필요합니다.

.단계
. 다운로드한 CSR 파일을 찾습니다.
+
다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

. CSR 파일을 CA(예: VeriSign 또는 DigiCert)에 제출하고 서명된 인증서를 PEM 형식으로 요청합니다.
+
[CAUTION]
====
* CSR 파일을 CA에 제출한 후에는 다른 CSR 파일을 다시 생성하지 마십시오. * CSR을 생성할 때마다 시스템은 개인 키 및 공개 키 쌍을 생성합니다. 공개 키는 CSR의 일부이며 개인 키는 시스템의 키 저장소에 보관됩니다. 서명된 인증서를 받아서 가져오면 시스템에서 개인 키와 공개 키가 모두 원래 쌍이 되도록 합니다. 키가 일치하지 않으면 서명된 인증서가 작동하지 않으므로 CA에서 새 인증서를 요청해야 합니다.

```
====
. CA가 서명된 인증서를 반환하면 로 이동합니다<<3단계: 관리 인증서를 가져옵니다>>.



== 3단계: 관리 인증서를 가져옵니다

CA(인증 기관)에서 서명된 인증서를 받은 후 웹 서비스 프록시 및 Unified Manager
인터페이스가 설치된 호스트 시스템으로 인증서를 가져옵니다.

.시작하기 전에
* CA로부터 서명된 인증서를 받았습니다. 이러한 파일에는 루트 인증서, 하나 이상의 중간 인증서
및 서버 인증서가 포함됩니다.
* CA가 체인 인증서 파일(예: .p7b 파일)을 제공한 경우, 루트 인증서, 하나 이상의 중간
인증서 및 서버 인증서 등 개별 파일에 체인 파일의 압축을 풀어야 합니다. Windows 유틸리티를
사용하여 파일의 압축을 풀 수 `certmgr` 있습니다(마우스 오른쪽 버튼을 클릭하고 메뉴: 모든
작업 [내보내기] 선택). base-64 인코딩이 권장됩니다. 내보내기가 완료되면 체인의 각 인증서
파일에 대해 CER 파일이 표시됩니다.
* 웹 서비스 프록시가 실행되고 있는 호스트 시스템에 인증서 파일을 복사했습니다.


.단계
. 인증서 관리 * 를 선택합니다.
. 관리 탭에서 * 가져오기 * 를 선택합니다.
+
인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

. 찾아보기 * 를 클릭하여 먼저 루트 및 중간 인증서 파일을 선택한 다음 서버 인증서를
선택합니다. 외부 도구에서 CSR을 생성한 경우 CSR과 함께 생성된 개인 키 파일도 가져와야
합니다.
+
대화 상자에 파일 이름이 표시됩니다.

. 가져오기 * 를 클릭합니다.


.결과
파일이 업로드되고 검증됩니다. 인증서 정보가 인증서 관리 페이지에 표시됩니다.



[[ID18b794e062706d9b6781f68002fb12e6]]
= 관리 인증서를 재설정합니다
:allow-uri-read:
:icons: font
```

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
관리 인증서를 공장 자체 서명된 원래 상태로 되돌릴 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.이 작업에 대해
이 작업은 Web Services Proxy 및 Unified Manager가 설치된 호스트 시스템에서 현재 관리 인증서를 삭제합니다. 인증서가 재설정되면 호스트 시스템은 자체 서명된 인증서를 사용하여 되돌아갑니다.

.단계
. 설정 > 인증서 * 를 선택합니다.
. Array Management * 탭을 선택한 다음 * Reset * 을 선택합니다.
+
관리 인증서 재설정 확인 대화 상자가 열립니다.

. 필드에 입력한 `reset` 다음 * 재설정 * 을 클릭합니다.
+
브라우저가 새로 고쳐지면 브라우저가 대상 사이트에 대한 액세스를 차단하고 사이트가 HTTP Strict Transport Security를 사용하고 있다고 보고할 수 있습니다. 이 조건은 자체 서명된 인증서로 다시 전환하면 발생합니다. 대상에 대한 액세스를 차단하는 조건을 지우려면 브라우저에서 탐색 데이터를 지워야 합니다.



.결과
시스템에서 서버에서 자체 서명된 인증서를 사용하도록 되돌립니다. 따라서 사용자가 세션에 대해 자체 서명된 인증서를 수동으로 수락하라는 메시지가 표시됩니다.



= 스토리지 인증서를 사용합니다

:leveloffset: +1


[[IDa7d6988ee95c2f18e6fceca19ffc8a21]]
= 스토리지에 대한 인증서를 가져옵니다
:allow-uri-read:
:experimental:
:icons: font
```

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
필요한 경우 Unified Manager를 호스팅하는 시스템에서 인증할 수 있도록 스토리지 어레이에 대한 인증서를 가져올 수 있습니다. 인증서는 CA(인증 기관)에서 서명할 수도 있고 자체 서명할 수도 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* 신뢰할 수 있는 인증서를 가져오는 경우 System Manager를 사용하여 스토리지 배열 컨트롤러에 대한 인증서를 가져와야 합니다.


.단계
. 인증서 관리 * 를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
+
이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.
+
보기를 제한하려면 * Show certificates that are... * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.

. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.
+
인증서가 업로드 및 검증됩니다.




[[ID4e88a37de08d9d44ad710d32d580f978]]
= 신뢰할 수 있는 인증서를 삭제합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
만료된 인증서와 같이 더 이상 필요하지 않은 인증서를 하나 이상 삭제할 수 있습니다.
```

.시작하기 전에
기존 인증서를 삭제하기 전에 새 인증서를 가져옵니다.

[CAUTION]
====
루트 또는 중간 인증서를 삭제하면 여러 스토리지 시스템이 동일한 인증서 파일을 공유할 수 있으므로 여러 스토리지 시스템에 영향을 줄 수 있습니다.

====
.단계
. 인증서 관리 * 를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
. 테이블에서 하나 이상의 인증서를 선택한 다음 * 삭제 * 를 클릭합니다.
+
[NOTE]
====
사전 설치된 인증서에는 * 삭제 * 기능을 사용할 수 없습니다.

====
+
신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.

. 삭제를 확인한 다음 * 삭제 * 를 클릭합니다.
+
인증서가 테이블에서 제거됩니다.

[[ID2f8d70dd2671303745104a79c6e59c48]]
= 신뢰할 수 없는 인증서를 확인합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
신뢰할 수 없는 인증서는 스토리지 어레이에서 Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다.

인증서 페이지에서는 스토리지 배열에서 자체 서명된 인증서를 가져오거나 신뢰할 수 있는 타사에서 발급한 CA(인증 기관) 인증서를 가져와 신뢰할 수 없는 인증서를 확인할 수 있습니다.

.시작하기 전에

* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
* CA 서명 인증서를 가져올 계획인 경우:
+
** 스토리지 배열의 각 컨트롤러에 대한 인증서 서명 요청(.csr 파일)을 생성하여 CA로 보냈습니다.
** CA가 신뢰할 수 있는 인증서 파일을 반환했습니다.
** 인증서 파일은 로컬 시스템에서 사용할 수 있습니다.

.이 작업에 대해
다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

* 최근에 스토리지 배열을 추가했습니다.
* 하나 이상의 인증서가 만료되었습니다.
* 하나 이상의 인증서가 해지되었습니다.
* 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
+
이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.
+
보기를 제한하려면 * Show certificates that are... * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.

. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.
+
인증서가 업로드 및 검증됩니다.

:leveloffset: -1

= 인증서를 관리합니다

:leveloffset: +1

[[ID01aa5cdd59beda9ea747987bc5da7cbc]]
= 인증서를 봅니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
인증서를 사용하는 조직, 인증서를 발급한 기관, 유효 기간 및 지문(고유 식별자)을 포함하는 인증서의 요약 정보를 볼 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 다음 탭 중 하나를 선택합니다.
+
** * 관리 * -- 웹 서비스 프록시를 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. Unified Manager에 안전하게 액세스할 수 있습니다.
** * 신뢰 * -- Unified Manager가 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.

. 인증서에 대한 자세한 내용을 보려면 해당 행을 선택하고 행 끝에 있는 줄임표를 선택한 다음 * 보기 * 또는 * 내보내기 * 를 클릭합니다.

[[IDcffd7c90250f6a3ac0a9f75eca891f9d]]
= 인증서를 내보냅니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
인증서를 내보내 전체 세부 정보를 볼 수 있습니다.

.시작하기 전에

내보낸 파일을 열려면 인증서 뷰어 응용 프로그램이 있어야 합니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 다음 탭 중 하나를 선택합니다.
+
** * 관리 * -- 웹 서비스 프록시를 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. Unified Manager에 안전하게 액세스할 수 있습니다.
** * 신뢰 * -- Unified Manager가 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.

. 페이지에서 인증서를 선택한 다음 행 끝에 있는 줄임표를 클릭합니다.
. 내보내기 * 를 클릭한 다음 인증서 파일을 저장합니다.
. 인증서 뷰어 응용 프로그램에서 파일을 엽니다.

:leveloffset: -1

:leveloffset: -1

= 액세스 관리

:leveloffset: +1

[[ID956d3a16bf753ae4caed25e21ef552d9]]
= 액세스 관리 개요
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management는 Unified Manager에서 사용자 인증을 구성하는 방법입니다.

== 어떤 인증 방법을 사용할 수 있습니까?

다음과 같은 인증 방법을 사용할 수 있습니다.

* * 로컬 사용자 역할 * -- 인증은 RBAC(역할 기반 액세스 제어) 기능을 통해 관리됩니다. 로컬 사용자 역할에는 미리 정의된 사용자 프로필과 특정 액세스 권한이 있는 역할이 포함됩니다.
* * 디렉터리 서비스 * -- 인증은 LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다.
* * SAML * -- 인증은 SAML 2.0을 사용하여 ID 공급자(IDP)를 통해 관리됩니다.

자세한 내용:

* xref:{relative_path}how-access-management-works-unified.html["액세스 관리 작동 방식"]
* xref:{relative_path}access-management-terminology-unified.html["Access Management(액세스 관리) 용어"]
* xref:{relative_path}permissions-for-mapped-roles-unified.html["매핑된 역할에 대한 권한"]
* xref:{relative_path}access-management-with-saml.html["SAML"]

== 액세스 관리를 구성하려면 어떻게 합니까?

SANtricity 소프트웨어는 로컬 사용자 역할을 사용하도록 사전 구성되어 있습니다. LDAP를 사용하려면 액세스 관리 페이지에서 LDAP를 구성할 수 있습니다.

자세한 내용:

* xref:{relative_path}access-management-with-local-user-roles-unified.html["로컬 사용자 역할을 사용하여 액세스 관리"]
* xref:{relative_path}access-management-with-directory-services-unified.html["디렉토리 서비스를 통한 액세스 관리"]
* xref:{relative_path}configure-saml.html["SAML를 구성합니다"]

= 개념

:leveloffset: +1

[[ID7999f269dbe9d716cbbcde25a26bc1ff]]
= 액세스 관리 작동 방식
:allow-uri-read:
:icons: font

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Access Management를 사용하여 Unified Manager에서 사용자 인증을 설정합니다.



== 구성 워크플로우

Access Management 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에
로그인합니다.
+
[NOTE]
====
처음 로그인하는 경우 사용자 이름이 `admin` 자동으로 표시되며 변경할 수 없습니다.
`admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다. 암호는 처음 로그인할 때 설정해야
합니다.

====
. 관리자는 미리 구성된 로컬 사용자 역할이 포함된 사용자 인터페이스에서 Access
Management로 이동합니다. 이러한 역할은 RBAC(역할 기반 액세스 제어) 기능 구현입니다.
. 관리자는 다음 인증 방법 중 하나 이상을 구성합니다.
+
** * 로컬 사용자 역할 * -- 인증은 RBAC 기능을 통해 관리됩니다. 로컬 사용자 역할에는 특정
액세스 권한을 가진 사전 정의된 사용자 및 역할이 포함됩니다. 관리자는 이러한 로컬 사용자
역할을 단일 인증 방법으로 사용하거나 디렉터리 서비스와 함께 사용할 수 있습니다. 사용자 암호
설정 이외의 구성은 필요하지 않습니다.
** * 디렉터리 서비스 * -- 인증은 LDAP(Lightweight Directory Access Protocol)
서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다.
관리자가 LDAP 서버에 연결한 다음 LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
** * SAML * -- 인증은 SAML(Security Assertion Markup Language) 2.0을 사용하여
ID 공급자(IDP)를 통해 관리됩니다. 관리자는 IdP 시스템과 스토리지 어레이 간의 통신을 설정한
다음 IdP 사용자를 스토리지 어레이에 포함된 로컬 사용자 역할에 매핑합니다.



. 관리자는 Unified Manager에 대한 로그인 자격 증명을 제공합니다.
. 사용자는 자격 증명을 입력하여 시스템에 로그인합니다. 로그인 중에 시스템은 다음과 같은
백그라운드 작업을 수행합니다.
+
** 사용자 계정에 대해 사용자 이름과 암호를 인증합니다.
** 할당된 역할에 따라 사용자의 권한을 결정합니다.
** 사용자에게 사용자 인터페이스의 기능에 대한 액세스 권한을 제공합니다.
** 상단 배너에 사용자 이름을 표시합니다.
```

== 기능은 Unified Manager에서 사용할 수 있습니다

기능에 대한 액세스는 사용자가 할당한 역할에 따라 달라집니다. 여기에는 다음이 포함됩니다.

* * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용할 수 없는 기능은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다.

[[IDa48bd056a5de43f4a1e7244eada2439e]]
= Access Management(액세스 관리) 용어
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Unified Manager에 액세스 관리 용어가 어떻게 적용되는지 알아보십시오.

[cols="25h,~"]
|===
| 기간 | 설명

a|
Active Directory를 클릭합니다
a|
AD(Active Directory)는 Windows 도메인 네트워크에 LDAP를 사용하는 Microsoft 디렉터리 서비스입니다.

a|
바인딩
a|
바인딩 작업은 클라이언트를 디렉토리 서버에 인증하는 데 사용됩니다. 일반적으로 바인딩에는 계정 및 암호 자격 증명이 필요하지만 일부 서버에서는 익명 바인딩 작업을 허용합니다.

a|
CA
a|
CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.

a|
인증서
a|
인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.

a|
LDAP를 지원합니다
a|
LDAP(Lightweight Directory Access Protocol)는 분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하면 다양한 응용 프로그램 및 서비스를 LDAP 서버에 연결하여 사용자의 유효성을 검사할 수 있습니다.

a|
RBAC
a|
역할 기반 액세스 제어(RBAC)는 개별 사용자의 역할에 따라 컴퓨터 또는 네트워크 리소스에 대한 액세스를 제어하는 방법입니다. Unified Manager에는 사전 정의된 역할이 포함되어 있습니다.

a|
SAML
a|
SAML(Security Assertion Markup Language)은 두 개체 간의 인증 및 승인을 위한 XML

기반 표준입니다. SAML을 사용하면 다중 요소 인증을 수행할 수 있습니다. 사용자는 ID를 입증하기 위해 두 개 이상의 항목(예: 암호 및 지문)을 제공해야 합니다. 스토리지의 내장된 SAML 기능은 ID 어설션, 인증 및 권한 부여에 대해 SAML2.0을 준수합니다.

a|
SSO
a|
SSO(Single Sign-On)는 하나의 로그인 자격 증명 세트로 여러 응용 프로그램에 액세스할 수 있는 인증 서비스입니다.

a|
웹 서비스 프록시
a|
표준 HTTPS 메커니즘을 통해 액세스를 제공하는 웹 서비스 프록시를 사용하면 관리자가 스토리지 시스템에 대한 관리 서비스를 구성할 수 있습니다. 프록시는 Windows 또는 Linux 호스트에 설치할 수 있습니다. Unified Manager 인터페이스는 웹 서비스 프록시에서 사용할 수 있습니다.

|===

[[ID94ab25b79bd099d7c2e7c6690259a2ae]]
= 매핑된 역할에 대한 권한
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
RBAC(역할 기반 액세스 제어) 기능에는 하나 이상의 역할이 매핑된 사전 정의된 사용자가 포함됩니다. 각 역할에는 Unified Manager의 작업에 액세스할 수 있는 권한이 포함됩니다.

역할은 다음과 같이 작업에 대한 사용자 액세스를 제공합니다.

* * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용자에게 특정 기능에 대한 권한이 없는 경우 해당 기능을 선택할 수 없거나 사용자 인터페이스에 표시되지 않습니다.

[[ID40b520a77f84ee99420cd1e22e9f33e5]]
= 로컬 사용자 역할을 사용하여 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
관리자는 Unified Manager에서 적용된 RBAC(역할 기반 액세스 제어) 기능을 사용할 수 있습니다. 이러한 기능을 "로컬 사용자 역할"이라고 합니다.

== 구성 워크플로우

로컬 사용자 역할은 시스템에서 사전 구성됩니다. 로컬 사용자 역할을 인증에 사용하려면 관리자가 다음을 수행할 수 있습니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 사용자 프로파일을 검토합니다. 사용자 프로필은 미리 정의되어 있으며 수정할 수 없습니다.
. 필요에 따라 관리자는 각 사용자 프로필에 대해 새 암호를 할당합니다.
. 사용자는 할당된 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증에 로컬 사용자 역할만 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 암호를 변경합니다.
* 암호의 최소 길이를 설정합니다.

* 사용자가 암호 없이 로그인할 수 있도록 허용합니다.

[[ID9796eecc38bd8167ead2a792f501b01b]]
= 디렉토리 서비스를 통한 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
관리자는 LDAP(Lightweight Directory Access Protocol) 서버와 Microsoft의 Active Directory와 같은 디렉터리 서비스를 사용할 수 있습니다.

== 구성 워크플로우

네트워크에서 LDAP 서버 및 디렉토리 서비스를 사용하는 경우 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 LDAP 서버에 대한 구성 설정을 입력합니다. 설정에는 도메인 이름, URL 및 바인딩 계정 정보가 포함됩니다.
. LDAP 서버가 보안 프로토콜(LDAPS)을 사용하는 경우 관리자는 LDAP 서버와 웹 서비스 프록시가 설치된 호스트 시스템 간의 인증을 위해 CA(인증 기관) 인증서 체인을 업로드합니다.
. 서버 연결이 설정되면 관리자는 사용자 그룹을 로컬 사용자 역할에 매핑합니다. 이러한 역할은 미리 정의되어 있으며 수정할 수 없습니다.
. 관리자는 LDAP 서버와 웹 서비스 프록시 간의 연결을 테스트합니다.
. 사용자는 할당된 LDAP/Directory 서비스 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증을 위해 디렉터리 서비스를 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 디렉토리 서버를 추가합니다.
* 디렉토리 서버 설정을 편집합니다.
* LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
* 디렉토리 서버를 제거합니다.
* 암호를 변경합니다.
* 암호의 최소 길이를 설정합니다.
* 사용자가 암호 없이 로그인할 수 있도록 허용합니다.

[[ID26fa6d7ec346d3da827be93a19e5e885]]
= SAML을 통한 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management의 경우 관리자는 스토리지에 포함된 SAML(Security Assertion Markup Language) 2.0 기능을 사용할 수 있습니다.

== 구성 워크플로우

SAML 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 System Manager의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 액세스 관리 아래의 * SAML * 탭으로 이동합니다.
. 관리자는 ID 공급자(IDP)와의 통신을 구성합니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 스토리지 시스템과의 통신을 구성하기 위해 관리자는 IDP 시스템에서 IDP 메타데이터 파일을 다운로드한 다음 Unified Manager를 사용하여 파일을 스토리지 어레이에 업로드합니다.
. 관리자는 서비스 공급자와 IDP 간의 신뢰 관계를 설정합니다. 서비스 공급자는 사용자 인증을 제어합니다. 이 경우 스토리지 배열의 컨트롤러는 서비스 공급자 역할을 합니다. 관리자는 Unified Manager를 사용하여 컨트롤러의 서비스 공급자 메타데이터 파일을 내보내어 통신을 구성합니다. 그런 다음 관리자는 IDP 시스템에서 메타데이터 파일을 IDP로 가져옵니다.
+

[NOTE]
====
또한 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하는지 확인해야 합니다.

====
. 관리자는 스토리지 어레이의 역할을 IDP에 정의된 사용자 속성에 매핑합니다. 이를 위해 관리자는 Unified Manager를 사용하여 매핑을 생성합니다.
. 관리자는 IDP URL에 대한 SSO 로그인을 테스트합니다. 이 테스트는 스토리지 배열 및 IDP가 통신할 수 있도록 보장합니다.
+
[CAUTION]
====
SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
. Unified Manager에서 관리자는 스토리지 어레이에 대해 SAML을 활성화합니다.
. 사용자는 SSO 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증을 위해 SAML을 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 새 역할 매핑을 수정하거나 작성합니다
* 서비스 공급자 파일을 내보냅니다

== 액세스 제한

SAML이 활성화된 경우 사용자는 기존 Storage Manager 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

또한 다음 클라이언트는 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

* 엔터프라이즈 관리 창(EMW)
* CLI(Command-Line Interface)
* SDK(소프트웨어 개발자 키트) 클라이언트
* 대역내 클라이언트
* HTTP 기본 인증 REST API 클라이언트
* 표준 REST API 끝점을 사용하여 로그인합니다

```
:leveloffset: -1


= 로컬 사용자 역할을 사용합니다

:leveloffset: +1


[[ID37981d553d217ad232de05a9176a1e78]]
= 로컬 사용자 역할을 봅니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
로컬 사용자 역할 탭에서 기본 역할에 대한 사용자 매핑을 볼 수 있습니다. 이러한 매핑은 Unified Manager용 웹 서비스 프록시에 적용된 RBAC(역할 기반 액세스 제어)의 일부입니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

.이 작업에 대해
사용자 및 매핑을 변경할 수 없습니다. 암호만 수정할 수 있습니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
+
사용자는 다음 표에 나와 있습니다.

+
** * admin * -- 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이 사용자는 모든 역할을 포함합니다.
** * 스토리지 * -- 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자에게는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다.
** * 보안 * -- 액세스 관리 및 인증서 관리를 포함한 보안 구성을 담당하는 사용자입니다. 이 사용자는 보안 관리자 및 모니터 역할을 포함합니다.
** * 지원 * -- 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자에게는 지원 관리자 및 모니터 역할이 포함됩니다.
** * monitor * -- 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자는 Monitor 역할만 포함합니다.
```

** * rw * (읽기/쓰기) -- 이 사용자는 스토리지 관리자, 지원 관리자 및 모니터 역할을 포함합니다.
** * ro * (읽기 전용) -- 이 사용자는 Monitor 역할만 포함합니다.

[[IDe1c4cfa21767b8180f14eb5070eeb97c]]
= 로컬 사용자 프로필에 대한 암호를 변경합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management에서 각 사용자의 사용자 암호를 변경할 수 있습니다.

.시작하기 전에
* 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
* 로컬 관리자 암호를 알아야 합니다.

.이 작업에 대해
암호를 선택할 때는 다음 지침을 염두에 두십시오.

* 새 로컬 사용자 암호는 최소 암호(보기/편집 설정)에 대한 현재 설정을 충족하거나 초과해야 합니다.
* 암호는 대/소문자를 구분합니다.
* 후행 공백은 암호가 설정되어 있을 때 암호에서 제거되지 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
* 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.

.단계
. 액세스 관리 * 를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
. 테이블에서 사용자를 선택합니다.
+
암호 변경 단추를 사용할 수 있게 됩니다.

. 암호 변경 * 을 선택합니다.
+
암호 변경 대화 상자가 열립니다.

. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 사용자가 시스템에 액세스하기 위해 암호를 입력하도록 확인란을 선택할 수 있습니다.
. 두 필드에 선택한 사용자의 새 암호를 입력합니다.
. 이 작업을 확인하려면 로컬 관리자 암호를 입력한 다음 * 변경 * 을 클릭합니다.

.결과
사용자가 현재 로그인한 경우 암호 변경으로 인해 사용자의 활성 세션이 종료됩니다.

[[IDda71f23b773e97a4f9302d33b5be0492]]
= 로컬 사용자 암호 설정을 변경합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
모든 신규 또는 업데이트된 로컬 사용자 암호에 필요한 최소 길이를 설정할 수 있습니다. 또한 로컬 사용자가 암호를 입력하지 않고 시스템에 액세스하도록 허용할 수 있습니다.

.시작하기 전에
루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.

.이 작업에 대해
로컬 사용자 암호의 최소 길이를 설정할 때는 다음 지침을 염두에 두십시오.

* 설정을 변경해도 기존 로컬 사용자 암호에는 영향을 주지 않습니다.
* 로컬 사용자 암호에 필요한 최소 길이 설정은 0자에서 30자 사이여야 합니다.
* 새 로컬 사용자 암호는 현재 최소 길이 설정을 충족하거나 초과해야 합니다.
* 로컬 사용자가 암호를 입력하지 않고 시스템에 액세스하도록 하려면 암호의 최소 길이를 설정하지 마십시오.

.단계
. 액세스 관리 * 를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
. 설정 보기/편집 * 을 선택합니다.
+
로컬 사용자 암호 설정 대화 상자가 열립니다.

. 다음 중 하나를 수행합니다.
+
** 로컬 사용자가 암호를 입력하지 않고 _시스템에 액세스할 수 있도록 하려면 "모든 로컬 사용자 암호를 최소한 입력해야 함" 확인란의 선택을 취소합니다.

** 모든 로컬 사용자 암호에 대해 최소 암호 길이를 설정하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란을 선택한 다음 spinner 상자를 사용하여 모든 로컬 사용자 암호에 필요한 최소 길이를 설정합니다.
+
새 로컬 사용자 암호는 현재 설정을 충족하거나 초과해야 합니다.

. 저장 * 을 클릭합니다.

:leveloffset: -1

= 디렉토리 서비스를 사용합니다

:leveloffset: +1

[[ID6e38a02877fa073480f81a8c00033d74]]
= 디렉토리 서버를 추가합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리에 대한 인증을 구성하려면 Unified Manager용 웹 서비스 프록시를 실행하는 호스트와 LDAP 서버 간의 통신을 설정해야 합니다. 그런 다음 LDAP 사용자 그룹을 로컬 사용자 역할에 매핑합니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
* 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
* 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

.이 작업에 대해
디렉토리 서버를 추가하는 과정은 2단계로 이루어집니다. 먼저 도메인 이름과 URL을 입력합니다. 서버에서 보안 프로토콜을 사용하는 경우 비표준 서명 기관이 서명한 경우 인증을 위해 CA

인증서도 업로드해야 합니다. 바인딩 계정에 대한 자격 증명이 있는 경우 사용자 계정 이름 및 암호를 입력할 수도 있습니다. 다음으로 LDAP 서버의 사용자 그룹을 로컬 사용자 역할에 매핑합니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 디렉터리 서비스 * 탭에서 * 디렉터리 서버 추가 * 를 선택합니다.
+
디렉토리 서버 추가 대화 상자가 열립니다.

. 서버 설정 * 탭에서 LDAP 서버의 자격 증명을 입력합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명


 a|
* 구성 설정 *


 a|
도메인
 a|
LDAP 서버의 도메인 이름을 입력합니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(_username_@_domain_)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.


 a|
서버 URL입니다
 a|
LDAP 서버에 액세스하기 위한 URL을 의 형식으로 `ldap[s]://*host*:*port*` 입력합니다.


 a|
인증서 업로드(선택 사항)
 a|

NOTE: 이 필드는 LDAPS 프로토콜이 위의 서버 URL 필드에 지정된 경우에만 나타납니다.

찾아보기 * 를 클릭하고 업로드할 CA 인증서를 선택합니다. LDAP 서버를 인증하는 데 사용되는 신뢰할 수 있는 인증서 또는 인증서 체인입니다.

a|
BIND ACCOUNT(선택 사항)
a|
LDAP 서버에 대한 검색 쿼리 및 그룹 내에서 검색할 읽기 전용 사용자 계정을 입력합니다. LDAP 유형 형식으로 계정 이름을 입력합니다. 예를 들어, 바인딩 사용자를 "bindacct"라고 하는 경우와 같은 값을 입력할 수 `CN=bindacct,CN=Users,DC=cpoc,DC=local` 있습니다.

a|
바인딩 암호(선택 사항)
a|

NOTE: 이 필드는 바인딩 계정을 입력할 때 나타납니다.

바인딩 계정의 암호를 입력합니다.

a|
추가하기 전에 서버 연결을 테스트합니다
a|
시스템이 입력한 LDAP 서버 구성과 통신할 수 있는지 확인하려면 이 확인란을 선택합니다. 이 테스트는 대화 상자 하단의 * 추가 * 를 클릭하면 발생합니다.

이 확인란을 선택하고 테스트에 실패하면 구성이 추가되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 추가할 수 있습니다.

a|
* 권한 설정 *

a|
검색 기준 DN
a|
사용자를 검색할 LDAP 컨텍스트를 입력합니다(일반적으로 의 형식 `CN=Users, DC=cpoc, DC=local`).

```
 a|
```
사용자 이름 특성입니다
```
 a|
```
인증을 위해 사용자 ID에 바인딩된 특성을 입력합니다. 예를 들면 다음과 `sAMAccountName`같습니다.

```
 a|
```
그룹 속성
```
 a|
```
그룹 대 역할 매핑에 사용되는 사용자의 그룹 속성 목록을 입력합니다. 예를 들면 다음과 `memberOf, managedObjects`같습니다.

```
|===
====
```
. 역할 매핑 * 탭을 클릭합니다.
. 미리 정의된 역할에 LDAP 그룹을 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
.필드 상세정보
```
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 매핑 *

 a|
그룹 DN
 a|
매핑할 LDAP 사용자 그룹의 그룹 DN(고유 이름)을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 정규식 패턴의 일부가 아닌 경우 백슬래시(\)로 이스케이프되어야 합니다. \. [] {}() <>*+-=!?^$|

 a|
역할
 a|
필드를 클릭하고 그룹 DN에 매핑할 로컬 사용자 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity Unified Manager에 로그인하려면 Monitor
```

역할이 다른 역할과 함께 필요합니다. 매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 매핑을 마쳤으면 * 추가 * 를 클릭합니다.
+
시스템은 스토리지 시스템 및 LDAP 서버가 통신할 수 있도록 검증을 수행합니다. 오류 메시지가 나타나면 대화 상자에 입력한 자격 증명을 확인하고 필요한 경우 정보를 다시 입력합니다.

[[ID03608d05a99d897137503109f4c4901c]]
= 디렉토리 서버 설정 및 역할 매핑을 편집합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
이전에 Access Management에서 디렉터리 서버를 구성한 경우 언제든지 해당 설정을 변경할 수 있습니다. 설정에는 서버 연결 정보와 그룹 대 역할 매핑이 포함됩니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 디렉토리 서버를 정의해야 합니다.

.단계
. 액세스 관리 * 를 선택합니다.

. 디렉터리 서비스 * 탭을 선택합니다.
. 둘 이상의 서버가 정의된 경우 테이블에서 편집할 서버를 선택합니다.
. 설정 보기/편집 * 을 선택합니다.
+
Directory Server Settings(디렉터리 서버 설정) 대화 상자가 열립니다.

. 서버 설정 * 탭에서 원하는 설정을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명


 a|
* 구성 설정 *


 a|
도메인
 a|
LDAP 서버의 도메인 이름입니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(_username_@_domain_)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.


 a|
서버 URL입니다
 a|
의 형식으로 LDAP 서버에 액세스하기 위한 URL `ldap[s]://host:port`입니다.


 a|
BIND ACCOUNT(선택 사항)
 a|
LDAP 서버에 대한 검색 쿼리 및 그룹 내 검색을 위한 읽기 전용 사용자 계정입니다.


 a|
바인딩 암호(선택 사항)
 a|

바인딩 계정의 암호입니다. (이 필드는 바인딩 계정을 입력할 때 나타납니다.)

a|
저장하기 전에 서버 연결을 테스트합니다
a|
시스템이 LDAP 서버 구성과 통신할 수 있는지 확인합니다. 테스트는 * 저장 * 을 클릭한 후에 수행됩니다. 이 확인란을 선택하고 검사에 실패하면 구성이 변경되지 않습니다. 테스트를 건너뛰고 구성을 다시 편집하려면 오류를 해결하거나 확인란을 선택 해제해야 합니다.

a|
* 권한 설정 *

a|
검색 기준 DN
a|
사용자를 검색하는 LDAP 컨텍스트(일반적으로 의 형식 `CN=Users, DC=cpoc, DC=local`)

a|
사용자 이름 특성입니다
a|
인증을 위해 사용자 ID에 바인딩된 속성입니다. 예를 들면 다음과 `sAMAccountName`같습니다.

a|
그룹 속성
a|
그룹-역할 매핑에 사용되는 사용자의 그룹 속성 목록입니다. 예를 들면 다음과 `memberOf, managedObjects`같습니다.

|===
====
. 역할 매핑 * 탭에서 원하는 매핑을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]

```
|===
| 설정 | 설명


 a|
* 매핑 *



 a|
그룹 DN
 a|
매핑할 LDAP 사용자 그룹의 도메인 이름입니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 정규식 패턴의 일부가 아닌 경우 백슬래시(\)로 이스케이프되어야 합니다.

\.[]{}() <> * +-=!?^$|



 a|
역할
 a|
그룹 DN에 매핑할 역할입니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity Unified Manager에 로그인하려면 Monitor 역할이 다른 역할과 함께 필요합니다. 역할은 다음과 같습니다.

** * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.



|===
====
+

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 저장 * 을 클릭합니다.



.결과
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.
```

```
[[ID2492221a0883c698517d9af4928c3565]]
= 디렉토리 서버를 제거합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
디렉터리 서버와 웹 서비스 프록시 간의 연결을 끊는 경우 Access Management 페이지에서 서버 정보를 제거할 수 있습니다. 새 서버를 구성한 다음 이전 서버를 제거하려는 경우 이 작업을 수행할 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

.이 작업에 대해
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 디렉터리 서비스 * 탭을 선택합니다.
. 목록에서 삭제할 디렉토리 서버를 선택합니다.
. 제거 * 를 클릭합니다.
+
디렉터리 서버 제거 대화 상자가 열립니다.

. 필드에 입력한 `remove` 다음 * 제거 * 를 클릭합니다.
+
디렉토리 서버 구성 설정, 권한 설정 및 역할 매핑이 제거됩니다. 사용자는 더 이상 이 서버의 자격 증명으로 로그인할 수 없습니다.




:leveloffset: -1


= SAML을 사용합니다

:leveloffset: +1
```

```
[[ID14c90a7005fe562c6693a14229cd7070]]
= SAML를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
액세스 관리에 대한 인증을 구성하려면 스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용할 수 있습니다. 이 구성은 ID 공급자와 스토리지 공급자 간의 연결을 설정합니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 스토리지 배열에 있는 컨트롤러의 IP 주소 또는 도메인 이름을 알아야 합니다.
* IDP 관리자가 IDP 시스템을 구성했습니다.
* IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
* 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클록이 동기화되도록 했습니다.
* IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 Unified Manager 액세스에 사용되는 로컬 시스템에서 제공됩니다.


.이 작업에 대해
IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다. 서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다. IDP와 스토리지 어레이 간의 연결을 설정하려면 이 두 엔터티 간에 메타데이터 파일을 공유합니다. 다음으로 IDP 사용자 엔터티를 스토리지 어레이 역할에 매핑합니다. 마지막으로 SAML을 활성화하기 전에 연결 및 SSO 로그인을 테스트합니다.

[NOTE]
====
* SAML 및 디렉토리 서비스 *. 디렉터리 서비스가 인증 방법으로 구성되어 있을 때 SAML을 설정하면 SAML이 Unified Manager의 디렉터리 서비스를 대체합니다. 나중에 SAML을 사용하지 않도록 설정하면 Directory Services 구성이 이전 구성으로 돌아갑니다.

====
[CAUTION]
====
```

* 편집 및 사용 안 함. * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
SAML 인증 구성은 다단계 절차입니다.

== 1단계: IDP 메타데이터 파일을 업로드합니다

IDP 연결 정보를 스토리지 어레이에 제공하기 위해 IDP 메타데이터를 Unified Manager로 가져옵니다. IDP 시스템은 인증 요청을 올바른 URL로 리디렉션하고 받은 응답을 검증하려면 이 메타데이터가 필요합니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
+
구성 단계의 개요가 페이지에 표시됩니다.

. IdP(ID 공급자 가져오기) 파일 * 링크를 클릭합니다.
+
ID 공급자 파일 가져오기 대화 상자가 열립니다.

. 로컬 시스템에 복사한 IDP 메타데이터 파일을 선택하여 업로드하려면 * 찾아보기 * 를 클릭합니다.
+
파일을 선택하면 IDP 엔티티 ID가 표시됩니다.

. 가져오기 * 를 클릭합니다.

== 2단계: 서비스 제공업체 파일 내보내기

IDP와 스토리지 어레이 간의 신뢰 관계를 설정하려면 서비스 공급자 메타데이터를 IDP로 가져옵니다. IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 서비스 공급자와 통신할 수 있도록 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

.단계
. Export Service Provider files *(서비스 제공자 파일 내보내기 *) 링크를 클릭합니다.
+
서비스 공급자 파일 내보내기 대화 상자가 열립니다.

. 컨트롤러 A * 필드에 컨트롤러 IP 주소 또는 DNS 이름을 입력한 다음 * 내보내기 * 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.
+
내보내기 * 를 클릭하면 서비스 공급자 메타데이터가 로컬 시스템에 다운로드됩니다. 파일이 저장된 위치를 기록해 둡니다.

. 로컬 시스템에서 내보낸 XML 형식의 서비스 공급자 메타데이터 파일을 찾습니다.
. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져와 트러스트 관계를 설정합니다. 파일을 직접 가져오거나 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.

== 3단계: 역할 매핑

사용자에게 Unified Manager에 대한 권한 부여 및 액세스 권한을 제공하려면 IDP 사용자 특성 및 그룹 멤버쉽을 스토리지 어레이의 사전 정의된 역할에 매핑해야 합니다.

.시작하기 전에
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* IDP 메타데이터 파일을 Unified Manager로 가져옵니다.
* 컨트롤러의 서비스 공급자 메타데이터 파일은 신뢰 관계를 위해 IDP 시스템으로 가져옵니다.

.단계
. Unified Manager * 역할 매핑 링크를 클릭합니다.
+
역할 매핑 대화 상자가 열립니다.

. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 매핑 *

 a|
사용자 속성

a|
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.

a|
속성 값
a|
매핑할 그룹의 속성 값을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다

a|
역할
a|
필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 포함할 각 역할을 개별적으로 선택해야 합니다. Monitor 역할은 Unified Manager에 로그인하기 위한 다른 역할과 함께 필요합니다. 하나 이상의 그룹에 보안 관리자 역할도 필요합니다.

매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+
[NOTE]
====
Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 모든 사용자는 Unified Manager가 올바르게 작동하지 않습니다.

====
. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
+
[NOTE]
====
역할 매핑은 SAML이 활성화된 후에 수정할 수 있습니다.

====
. 매핑을 마치면 * 저장 * 을 클릭합니다.

== 4단계: SSO 로그인을 테스트합니다

IDP 시스템 및 스토리지 어레이가 통신할 수 있도록 SSO 로그인을 선택적으로 테스트할 수 있습니다. 이 테스트는 SAML을 활성화하기 위한 마지막 단계에서도 수행됩니다.

.시작하기 전에
* IDP 메타데이터 파일을 Unified Manager로 가져옵니다.
* 컨트롤러의 서비스 공급자 메타데이터 파일은 신뢰 관계를 위해 IDP 시스템으로 가져옵니다.

.단계
. Test SSO Login * 링크를 선택합니다.
+
SSO 자격 증명을 입력하기 위한 대화 상자가 열립니다.

. 보안 관리자 권한과 모니터 권한이 모두 있는 사용자의 로그인 자격 증명을 입력합니다.
+
시스템에서 로그인을 테스트하는 동안 대화 상자가 열립니다.

. 테스트 성공 메시지를 찾습니다. 테스트가 성공적으로 완료되면 SAML 활성화를 위한 다음 단계로 이동합니다.
+
테스트가 성공적으로 완료되지 않으면 추가 정보와 함께 오류 메시지가 나타납니다. 다음을 확인합니다.

+
** 사용자는 보안 관리자 및 모니터 권한이 있는 그룹에 속합니다.
** IDP 서버에 대해 업로드한 메타데이터가 정확합니다.
** SP 메타데이터 파일의 컨트롤러 주소가 올바릅니다.

== 5단계: SAML을 활성화합니다

마지막 단계는 사용자 인증을 위해 SAML 구성을 완료하는 것입니다. 이 프로세스 중에 SSO 로그인을 테스트하라는 메시지가 표시됩니다. SSO 로그인 테스트 프로세스는 이전 단계에서 설명합니다.

.시작하기 전에
* IDP 메타데이터 파일을 Unified Manager로 가져옵니다.
* 컨트롤러의 서비스 공급자 메타데이터 파일은 신뢰 관계를 위해 IDP 시스템으로 가져옵니다.
* 하나 이상의 Monitor 및 Security Admin 역할 매핑이 구성되어 있습니다.

[CAUTION]
====
* 편집 및 사용 안 함. * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
.단계
. SAML * 탭에서 * SAML * 활성화 링크를 선택합니다.
+
Confirm Enable SAML(SAML 활성화 확인) 대화 상자가 열립니다.

. 을 입력하고 `enable` * 사용 * 을 클릭합니다.
. SSO 로그인 테스트에 대한 사용자 자격 증명을 입력합니다.

.결과
시스템에서 SAML을 활성화하면 모든 활성 세션이 종료되고 SAML을 통해 사용자 인증이 시작됩니다.

[[IDa0d8bb04d1036f92a4a4e7492126eae3]]
= SAML 역할 매핑을 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
이전에 Access Management에 SAML을 구성한 경우 IDP 그룹과 스토리지 배열의 사전 정의된 역할 간의 역할 매핑을 변경할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* SAML이 구성 및 활성화되었습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
. 역할 매핑 * 을 선택합니다.
+
역할 매핑 대화 상자가 열립니다.

. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
[CAUTION]
====
SAML이 활성화되어 있는 동안에는 권한을 제거하지 않도록 주의하십시오. 그렇지 않으면 Unified Manager에 액세스할 수 없게 됩니다.

====
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

a|
* 매핑 *

a|
사용자 속성
a|
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.

a|
속성 값
a|
매핑할 그룹의 속성 값을 지정합니다.

a|

역할
 a|
필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. Monitor 역할은 Unified Manager에 로그인하기 위한 다른 역할과 함께 필요합니다. 보안 관리자 역할은 하나 이상의 그룹에 할당해야 합니다. 매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 모든 사용자는 Unified Manager가 올바르게 작동하지 않습니다.

. 선택적으로 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 저장 * 을 클릭합니다.

.결과
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

[[ID8aca846bcb4883e5e362b8f162032547]]
= SAML 서비스 공급자 파일을 내보냅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
필요한 경우 스토리지 배열에 대한 서비스 공급자 메타데이터를 내보내고 해당 파일을 IdP(Identity Provider) 시스템으로 다시 가져올 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* SAML이 구성 및 활성화되었습니다.

.이 작업에 대해
이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다. IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 요청을 보내는 데 사용할 수 있는 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
. 내보내기 * 를 선택합니다.
+
서비스 공급자 파일 내보내기 대화 상자가 열립니다.

. 내보내기 * 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.
+
[NOTE]
====
도메인 이름 필드는 읽기 전용입니다.

====
+
파일이 저장된 위치를 기록해 둡니다.

. 로컬 시스템에서 내보낸 XML 형식의 서비스 공급자 메타데이터 파일을 찾습니다.
. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져옵니다. 파일을 직접 가져오거나 컨트롤러 정보를 수동으로 입력할 수 있습니다.
. 닫기 * 를 클릭합니다.

:leveloffset: -1

= FAQ 를 참조하십시오

:leveloffset: +1

[[IDdfec7854ce0487db07a0721a0820c449]]
= 로그인할 수 없는 이유는 무엇입니까?
:allow-uri-read:

```
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
로그인을 시도할 때 오류가 발생하면 다음과 같은 가능한 원인을 검토하십시오.

다음과 같은 이유 중 하나로 인해 로그인 오류가 발생할 수 있습니다.

* 잘못된 사용자 이름 또는 암호를 입력했습니다.
* 권한이 부족합니다.
* 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 다시 로그인하려면 10분 정도 기다립니다.
* SAML 인증이 활성화되었습니다. 로그인하려면 브라우저를 새로 고치십시오.




[[IDadbfb038045ef1086e3dfa247e39ba30]]
= 디렉토리 서버를 추가하기 전에 알아야 할 사항은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Access Management에서 디렉터리 서버를 추가하기 전에 특정 요구 사항을 충족해야 합니다.

* 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
* 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
* 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.




[[ID66814e05e9e6712f4442210e1b68cc93]]
= 스토리지 어레이 역할에 매핑하는 방법에 대해 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
그룹을 역할에 매핑하기 전에 지침을 검토하십시오.

RBAC(역할 기반 액세스 제어) 기능에는 다음 역할이 포함됩니다.

* * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

[NOTE]
====
Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

====
LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스를 사용하는 경우 다음 사항을 확인하십시오.

* 관리자가 디렉토리 서비스에 사용자 그룹을 정의했습니다.
* LDAP 사용자 그룹의 그룹 도메인 이름을 알고 있습니다.

== SAML

스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하는 경우 다음 사항을 확인하십시오.

* IDP(Identity Provider) 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* 그룹 구성원 이름을 알고 있습니다.
* 매핑할 그룹의 속성 값을 알고 있습니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다.
+
[listing]
----
\.[]{}()<>*+-=!?^$|
----
* Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 모든 사용자는 Unified Manager가 올바르게 작동하지 않습니다.

```
[[IDd5b0e600ad81924e8a997d88eee1b146]]
= SAML을 구성 및 활성화하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증을 위해 SAML(Security Assertion Markup Language) 기능을 구성 및 활성화하기 전에 다음 요구 사항을 충족하고 SAML 제한 사항을 이해해야 합니다.



== 요구 사항

시작하기 전에 다음 사항을 확인하십시오.

* ID 공급자(IDP)가 네트워크에 구성되어 있습니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹을 구성했습니다.
* IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
* 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클록이 동기화되도록 했습니다.
* IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 Unified Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.
* 스토리지 배열의 컨트롤러에 있는 IP 주소 또는 도메인 이름을 알고 있습니다.



== 제한 사항

위의 요구 사항 외에 다음과 같은 제한 사항을 이해해야 합니다.

* SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오. 최종 구성 단계에서 SAML을 활성화하기 전에 SSO 로그인을 테스트하는 것이 좋습니다. (SAML을 활성화하기 전에 SSO 로그인 테스트도 수행합니다.)
* 나중에 SAML을 사용하지 않도록 설정하면 이전 구성(로컬 사용자 역할 및/또는 디렉터리 서비스)이 자동으로 복원됩니다.
* 디렉토리 서비스가 현재 사용자 인증을 위해 구성된 경우 SAML은 해당 구성을 재정의합니다.
* SAML이 구성된 경우 다음 클라이언트가 스토리지 시스템 리소스에 액세스할 수 없습니다.
+
```

** 엔터프라이즈 관리 창(EMW)
** CLI(Command-Line Interface)
** SDK(소프트웨어 개발자 키트) 클라이언트
** 대역내 클라이언트
** HTTP 기본 인증 REST API 클라이언트
** 표준 REST API 끝점을 사용하여 로그인합니다

[[ID7e7c8d5a00cb52dc0d6de221a4410ba5]]
= 로컬 사용자는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
로컬 사용자는 시스템에 미리 정의되어 있으며 특정 권한을 포함합니다.

로컬 사용자는 다음과 같습니다.

* * admin * -- 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이 사용자는 모든 역할을 포함합니다. 암호는 처음 로그인할 때 설정해야 합니다.
* * 스토리지 * -- 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자에게는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * 보안 * -- 액세스 관리 및 인증서 관리를 포함한 보안 구성을 담당하는 사용자입니다. 이 사용자는 보안 관리자 및 모니터 역할을 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * 지원 * -- 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자에게는 지원 관리자 및 모니터 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * monitor * -- 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자는 Monitor 역할만 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * rw * (읽기/쓰기) -- 이 사용자는 스토리지 관리자, 지원 관리자 및 모니터 역할을 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * ro * (읽기 전용) -- 이 사용자는 Monitor 역할만 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.

:leveloffset: -1

```
:leveloffset: -1


:leveloffset: -1


:leveloffset: -1

<<<
```

DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

*상표 정보*

NETAPP, NETAPP 로고 및
link:http://www.netapp.com/TM[http://www.netapp.com/TM^]에 나열된 마크는
NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.